1-1-2011

Design And Evaluation Of Laboratory Practices For An Advanced Computer Networking Curriculum

Jorgealberto Zetino
Eastern Illinois University

THESIS MAINTENANCE AND REPRODUCTION CERTIFICATE

TO: Graduate Degree Candidates (who have written formal theses)

SUBJECT: Permission to Reproduce Theses

The University Library is receiving a number of request from other institutions asking permission to reproduce dissertations for inclusion in their library holdings. Although no copyright laws are involved, we feel that professional courtesy demands that permission be obtained from the author before we allow these to be copied.

PLEASE SIGN ONE OF THE FOLLOWING STATEMENTS:

Booth Library of Eastern Illinois University has my permission to lend my thesis to a reputable college or university for the purpose of copying it for inclusion in that institution's library or research holdings.

[signature] May 7th 2011

Author's Signature Date

I respectfully request Booth Library of Eastern Illinois University **NOT** allow my thesis to be reproduced because:

_____

_____

_____

_____ _____

Author's Signature Date

This form must be submitted in duplicate.

Design and Evaluation of Laboratory Practices for an Advanced Computer Networking Curriculum

(TITLE)

BY

Jorgealberto Zetino

THESIS

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF

Master of Science in Technology

IN THE GRADUATE SCHOOL, EASTERN ILLINOIS UNIVERSITY
CHARLESTON, ILLINOIS

2011

YEAR

I HEREBY RECOMMEND THAT THIS THESIS BE ACCEPTED AS FULFILLING
THIS PART OF THE GRADUATE DEGREE CITED ABOVE

5/05/11	5/9/11
THESIS COMMITTEE CHAIR — DATE	DEPARTMENT/SCHOOL CHAIR OR CHAIR'S DESIGNEE — DATE
THESIS COMMITTEE MEMBER — DATE	THESIS COMMITTEE MEMBER — DATE
5/05/11	5/05/11
THESIS COMMITTEE MEMBER — DATE	THESIS COMMITTEE MEMBER — DATE

Design and Evaluation of Laboratory Practices for

an Advanced Computer Networking Curriculum

(TITLE)

BY

Jorgealberto Zetino

THESIS

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF

Master of Science in Technology

IN THE GRADUATE SCHOOL, EASTERN ILLINOIS UNIVERSITY
CHARLESTON, ILLINOIS

2011

YEAR

I HEREBY RECOMMEND THAT THIS THESIS BE ACCEPTED AS FULFILLING
THIS PART OF THE GRADUATE DEGREE CITED ABOVE

5/05/2011	Deborah A Woodley 5/9/11
THESIS COMMITTEE CHAIR — DATE	DEPARTMENT/SCHOOL CHAIR OR CHAIR'S DESIGNEE — DATE
THESIS COMMITTEE MEMBER — DATE	THESIS COMMITTEE MEMBER — DATE
Samuel Sheets 5/05/11	5/05/11
THESIS COMMITTEE MEMBER — DATE	THESIS COMMITTEE MEMBER — DATE

Design and Evaluation of Laboratory Practices for an Advanced Computer Networking Curriculum

Jorgealberto Zetino

Eastern Illinois University

April 20, 2011

Abstract

Educators in the area of computer networking face the challenge of developing successful academic courses that can increase students' comprehension and interest while improving their competitiveness in the job market. This situation requires the development of a curriculum with emphasis on current industry needs and practical activities that can provide students with hands-on experience. This study focuses on the development of laboratory practices in three areas of significant importance for the industry: network security, wireless networks and voice over IP. The objectives of the laboratory practices are to improve the use of equipment in the telecommunication laboratory at Eastern Illinois University, to provide additional theoretical background for the students, to provide easy to understand procedures and to present scenarios that closely resemble real life situations. These practices might be added to the current curriculum in computer networking or used as a basis for the development of a new and more comprehensive curriculum.

Keywords: computer networking, laboratory, network security, wireless, voice over IP.

Acknowledgments

I take this opportunity to express my deepest gratitude to my thesis advisor and supervisor Dr. Rigoberto Chinchilla, it was thanks to his help and guidance that I was able to start and complete this master program.

I would also like to thank my thesis committee members Dr. Rendong Bai and Dr. Samuel Guccione for their guidance through the completion of my thesis.

Finally, I thank my family for their love and support through all this years, and particularly through the time that I spend at Eastern Illinois University working on my Master's Degree.

Table of Contents

List of Figures

The following is a list of the figures presented within the main document. This list does not include figures presented in the Appendices.

Chapter 1

Introduction

This chapter discusses the purpose and importance of this study and the reasons that support the development of laboratory practices in the area of computer networks; starting from the importance of the field and the different challenges that industry and educators need to overcome.

The adoption of computer networks as a new way for data interchange during the nineties drastically changed the way companies work. Gauchi (1995) referred to this situation indicating that "the real change in organization mindset began when computers were hooked to one another to transfer information seamlessly between departments, functions, and companies". Over recent years, new technologies have allowed the development of two areas of considerable importance: wireless networks and converged networks. These new developments bring more concerns to the network administrator, not only in terms of implementing these technologies, but also in terms of security, management and the assurance of scalability. The implementation of new technologies requires the network administrators to go beyond the basics, raising the need for a more elaborated educational curriculum in the area of computer networks.

From an academic stand point, the teaching of computer networks and other topics in telecommunications represent a challenge for the instructor: Sarkar (2006) indicated that students might find the subject too technical and sometimes boring, stating that students learn more effectively when courses include practical activities; Rickman, M. McDonald, G. McDonald and Heeler(2001) highlight the need of a practical curriculum more accommodated to the industry needs; yet Sarkar (2006) indicated that

"only a limited amount of material designed to supplement the teaching of computer networking is publicly available". This situation raises the need for instructors to design their own supplement material to provide the practical aspects of the subject to students.

Statement of the Problem

In a medium to small company environment, managing and securing the network might not present a problem, but as new services are added and other services become integrated in the data network, the management of the new converged network might become a challenge to the network administrator. Students intending to follow a career in the area of computer networks might present needs in three particular areas:

1. Additional theoretical background in concepts that are not fully covered in an introductory course.
2. Additional laboratory work.
3. Internship that will allow students to directly experience problems related to network management. (Rickman et al., 2001)

Rickman et al. (2001) also indicated that companies are looking not only for graduates that understand the concepts of networking but for people who can quickly be involved in the administration of the network. The School of Technology at Eastern Illinois University, with the goal of integrating people and technology to increase work performance in organizations, and its commitment for technological innovation, must provide students with an appropriate insight into the technologies currently used by the industry.

The development of comprehensive laboratory procedures and their integration in the learning curriculum is necessary to ensure the compliance with the employers needs

and to strengthen the concepts acquired during the lectures. Since the current physical topology of the telecommunication laboratory of the School of Technology presents a problem in terms of resource utilization, it is necessary to redesign it in order to improve the use of resources and the teaching of concepts in different areas of computer networking. From this problem statement we can formulate a hypothesis that will provide a solution to this issue.

Hypothesis

The development of new laboratory practices will allow a better teaching of different areas of computer networking and improve the use of equipment in the telecommunication laboratory of The School of Technology at EIU.

Statement of Purpose

Based on the hypothesis, the purpose of this study is the design of methodologies in the form of laboratory practices for the deployment of a network that exemplifies the current industry needs; covering basic implementations of wireless LANs (WLAN) and VoIP infrastructures, as well as different solutions in the area of network security, particularly in the form of centralized authentication.

Using the equipment from the Telecommunications Laboratory of the School of Technology, student will be guided by means of the different practices in the process of transforming a simple wired network into a converged network with a centralized security management. The laboratory practices can be included in a new intermediate level course in computer networks, or integrated as standalone practices in already existing courses in the area of data communication for either undergraduate or graduate students in order to enhance the existing curriculum in the area. The development of

these laboratory procedures intends to provide a solution to the theoretical background and laboratory work needs previously presented, while providing a basis for students that are preparing to enter an internship in the area of computer networks.

Objectives

The overall study will be focused in accomplishing the following objectives:

1. To provide an additional theoretical background for the student in the area of computer networks by the implementation of laboratory practices.
2. To develop comprehensive and easy to understand laboratory procedures for students in the area of computer networks.
3. To develop laboratory practices in a way that allows the student to identify similarities with real life situations.
4. To enhance the use of the laboratory equipment in a way that integrates all the devices, allowing the students to get practical experience in the use of different technologies.

The proper configuration of the laboratory equipment and the development of the different laboratory practices must lead to the achievement of the previously established objectives and the statement of purpose.

Delimitations

The laboratory practices will use the telecommunications laboratory equipment. Hence, the concepts to be presented in the laboratory practices will be under the limitation of the hardware, software and licensing capabilities. The students involved in the evaluation of the practice have entry to mid level knowledge in the area of computer networking.

Chapter 2

Literature Review

The previous chapter discussed the need to optimize the computer networking curriculum by developing laboratory practices that address the different industry needs. This chapter provides theoretical material that justifies the development of laboratory procedures in three particular areas of computer networking that have significant importance in the industry, as well as a theoretical basis of the different concepts that will be covered in the laboratory practices.

While the scope of the areas of wireless and voice technologies could be extended to develop more practices and to go in further details, equipment and time constrains limit the amount of practices and topics that can be covered in these two areas an introductory level. Appendix A contains a list with definitions of the different terms addresses in this document.

Description of Problem Area

While Rickman et al. (2001) addressed the need for educators to provide a curriculum in touch with the industry needs; Tang, Draper and Xu (2008) also indicated the importance of an adaptive laboratory that can be used for different learning objectives. Since adaptability in the telecommunication laboratory is limited by the equipment available, it is important to identify the significant areas that can addressed in an educational curriculum.

Theoretical Background Based in Industry Needs.

Based on industry needs, three areas can be highlighted as particularly significant. The first of these areas is network security, which has progressively increased its

importance in the last years, Paulson (2002) referred to this trend as early as 2002, while the Association for Computing Machinery [ACM] (2008, p. 61) presented Network Security as a core course of the Net Centric Computing area of its latest recommended Computer Science curriculum. The second area to be addressed comes in the form of mobile computing, which was presented as an elective course in the ACM curriculum (ACM, 2008, p.63), highlighting the impact that the emergence of wireless networks has provided to the industry, including benefits in terms of mobility, installations and reliability among other things (Geier, 2010, p. 15-18). Finally, the third area of interest is the incorporation of technologies such as voice and video over the existing network infrastructure, a trend that has gained significant popularity, and gave birth to the phenomenon known as network convergence (Hens & Caballero, 2008, p. 4), providing a significant advantage to businesses in terms of less expensive phone services as well as new business strategies and market opportunities for telecommunication companies. Other indicator of the importance of network security, mobile computing and network convergence in the form of voice over IP (VoIP), is the separation of the popular CCNA industry certification in paths that address one of these particular areas.

Based on equipment capabilities, the telecommunication laboratory offers the opportunity to address several concepts in the form of practical applications related to network security tools and strategies, mobile computing in the form of wireless local area networks (WLANs), as well as general implementation of VoIP. This is of particular importance in the case of a school of technology which intends to address the topic of computer networks from a standpoint of application and management of these technologies.

Laboratory Work.

The need of a laboratory in the area of computer networks comes from the fact that practical experience is a must in the field of computer networks, particularly when addressing the area of network security. Gregg (2008, p. 2) addressed this issue indicating that "a laboratory is as vital to a computer-security specialist as one is to a chemist or biologist", indicating that for the security professional, it is necessary to have a proper understanding about how these technologies will behave at different levels.

From an educational related standpoint, Rickman et al. (2001) indicated the need for both internships and laboratory for undergraduate students as a mean to gain practical experience in the area of networking and proposed a solution to this issue while indicating different areas where experience was desirable in order for students to be able to start a career in computer networking. Sarkar and Craig (2006) when referring to the teaching of fundamental concepts in the area of wireless, indicated that the teaching of wireless communication and networking is challenging since students might find the subjects too dry and technical, therefore, the development of projects that can catch the interest of the students and at the same time provide them with hands-on experience becomes particularly important.

A well designed laboratory is not only important for the students that need to acquire particular concepts in an area of computer networks; it also plays a major role in understanding the way that different technologies work from the basics. Gregg (2008, p. 3) indicated that even though there are many manuals that explain how different devices work, they cannot explain the way that different products will behave once they are combined in a complex network; particularly new technologies.

Resources Optimization in the Telecommunication Laboratory

One of the main objectives of this study is to enhance the use of the resources available in the Telecommunication Laboratory of the School of Technology. There is not a single way to address this problem, as there are many possible physical network topologies that can be built with the equipment available, ranging from simple to complex designs. The current computer network of the telecommunication laboratory is designed to address the basic networking concepts. Currently, the network experiences different changes as new devices are connected and other devices are disconnected from the topology as new practices are implemented.

The proposed topology aims to reduce the need of modifying the physical interconnections between devices, focusing on implementing step by step new network segment for the purpose of teaching more complex topics in the area of computer networks. The new topology considers the idea of a intermediate to advanced level course that follows each of the laboratory practices in an orderly manner and changes the laboratory topology accordingly, starting with the existing topology and adding a new segment that will increase in complexity by each practice implemented by the students. This new segment will be interconnected to the elements of the previous network in a way that exemplifies the growth of a network inside a company, with the implementation of new services and new challenges for the network administrator.

Covered Topics in Data Communication

Kasera, N. Narang and S. Narang (2007) established three subdivisions of advanced concepts that need to be addressed in order to provide a further insight in the field of networking:

1. Traffic management: Deals with the proper utilization of network resources and plays a significant role in converged networks and indirectly affects scalability.
2. Network management: Is concerned with the monitoring and modification of network operations and is considerably important when dealing with scalability issues.
3. Security management: Is concerned with confidentiality, integrity and availability of the data during the information exchange (p. 256-257).

These three subdivision overlap with the areas of interest for the industry presented early in this chapter; it can be observed that the areas of network security and security management share common characteristics, while the areas of mobile computing and network convergence cover topics from the three sections. While having a curriculum addressing the three areas presented by Kasera et al. (2007, p. 256-257) might be a good approach for an advanced course in computer networks, equipment availability and the scope of this study, focused on practical applications of technology, won't permit the addressing of each section directly in stand alone practices, with the exception of security management. For these reasons it was decided to take an approach based on the previously discussed areas of interest for the industry while still providing some references to the advanced concepts approach. Concepts to be covered in these areas will be further defined in the following sections.

Network security.

The importance of network security can be asserted after considering the way that information moves freely from place to place by means of computer networks. Burgess (2000) addressed the issue of network security by saying that "One [*sic*] a computer is

attached to the Internet, we have to consider the consequences of being connected to all other computers of the world" (p. 3). While the information travels within a network or the Internet, it might become vulnerable to interception, modification and even elimination; as Biggs (2004) stated, "the only safe computer is one that's completely disconnected from the Internet" (p. 133), but nowadays, the flow of information is equivalent to the flow of money. Companies are unable to keep their information shut in a safe where no one can see it; people demand the capability to access their information anytime anywhere.

Starting from the basics, Parker (2008) indicated that a security analyst shares many of the core skills of a network administrator, including (a) knowledge of major protocols, (b) network architecture concepts, and (c) project management experience among other things. Knowledge of protocols are a basic for the handling of firewalls and Access Control Lists (ACLs), while network architecture concepts allow the computer networks students to properly define the layout of the network and establish common practices to secure the network perimeter, and from that, create a layered defense strategy for the whole network. Based on equipment capabilities, the laboratory practices in the area of network security cover technologies such as ACLs, Networks Address Translation (NAT), Port Address Translation (PAT), Virtual Private Networks and different mechanisms for authentication. The laboratory practices focus on the implementation of these technologies providing a practical scenario for their application.

Demilitarized zone (DMZ).

A good example that gives a basic idea of how different security technologies can be applied in a real life scenario comes in the form of a DMZ, also known as perimeter

network. Under a layered approach to network defense, one of the most common practices is the implementation of a DMZ (Deal, 2002, p. 39); not only providing an example of the use of security technologies such as firewalls, ACLs and NAT, but as indicated by Parker (2008), an example of the use of network architecture skills.

While a DMZ can be set within the internal network of a company, it is usually a common practice for the establishment of a secure perimeter; in this way a DMZ can be defined as a network with a medium security level that stands between a network with a high-security level, usually an internal network, and a network with a low-security level, usually an external network as indicated by Thomas II, Freeland, Coker, and Stoddard (2001, p. 524)

Although other devices such as routers or servers can be used, a firewall is usually the base component of a DMZ, effectively dividing the network into different areas with a security level assigned to each one of them. Usually, traffic flows freely from a high-security level segment to a low-security level segment, while its flow between segments of the same security level and from low to high is regulated. ACLs work as rules that define which type of traffic is to be allowed between these areas. Deal (2002, p. 41) indicated that there are different ways to implement a DMZ, being a common approach the use of a single firewall for traffic segmentation.

Virtual private network (VPN).

The implementation of a secure perimeter for the internal network is just the starting point in the road of network security. This section covers the concept of VPN, its importance and other details.

From an academic standpoint, ACM (2008, p. 6) included VPN among the basic network defense tools and strategies that need to be addressed in a network security course, this is accompanied with concepts in the area of cryptography and the Internet Protocol Security (IPSec) suite. From an industry standpoint, as a company scope increases, employees and outsourcers, might find themselves in the need to access corporate resources outside of the network boundaries, which again highlights the importance of VPNs.

According to statistics, "90 percent of employees work away from their company's headquarters and 40 percent work at a remote location, away from their supervisors" (Turban, Leiden, McLean, & Wetherbe, 2008, p. 135), this gives rise to an increased concern in services availability and also to a new set of security concerns that need to be addressed in the security model of the network and leads to the conclusion that remote access to the resources of a company from outside the secured perimeter is a key concern for the security professional. Thomas II et al (2001) stated this situation as follow:

> With the explosion in network applications as businesses depend upon network services and availability, the need to protect not only network and data, but also the network from the *denial of services* (DoS) is emerging fast. Access control policies are formed by corporate policies [*sic*] that define the type of access that is allowed across an organization. A secure network model should not only take into account the border network perimeter, but the entire organization's network perimeter. (p. 183)

The problem arises when legitimate users need access to the resource of the company but they are using infrastructure outside of the company's network. VPN technologies solve the need of a secure channel for private traffic over a public infrastructure (Bhaiji, 2008, 423), allowing remote users access to services and resources within the company.

Since the corporate network is inevitably extended outside the company, the system administrator needs to establish a set of policies and measures in order to control remote access. Fung (2005, p. 153), when speaking about network security architectures, actually defined a remote access architecture that intends to set standards for implementation, and later stated that "there are no formal standards defined specifically to restrict what the Remote Access Architecture should exactly be like because different corporations or organizations have different remote access requirements" (p. 156). Nevertheless, it is possible to make a separation of remote access systems through VPN in three categories:

1. Access VPNs, which provide secure communication for remote users and the company network. This category is commonly known as remote-access VPN.
2. Intranet VPNs, which interconnect different locations of a company over a secure link. This type of VPN follows the configuration known as site-to-site VPN.
3. Extranet VPNs, which might provide a secure connection between customer, business partners or suppliers over a shared infrastructure. This category follow the site-to-site VPN configuration with the difference that access to the network resources is controlled in both ends. (Gibbs, Bastien. Carter & Degu, 2006, p. 331)

The current laboratory equipment capabilities allow the implementation of both site-to-site VPNs in the form of an Intranet VPN and the remote-access VPN. While there are different ways to establish a VPN connection the study will focus on IPSec, currently one of the most widely used VPN mechanisms, providing examples of its application and the way it interacts with the different data encryption standards and hashing mechanisms for data integrity, addressing the way that they work together to establish a bidirectional secure association between different peers.

Centralized network access control.

The final concept in the area of network security that will be covered in this study as a stand-alone topic is the use of centralized authentication for network access control. The importance of this topic and other details will be further explained in this section.

The implementation of different methods to access the corporate network and its devices, as well as the security measures established to control them, can make the management of users credentials a complex process with several negative consequences for the network administrator. Fung (2005) described this problem, indicating that "one of the biggest headaches and sources of problems with remote access security has been the need to manage the many different components on a server-by-server basis". (p. 154)

A network that handles VPN access, access to WLAN, and administrative access to network devices in a decentralized way, with users' credentials stored in different databases might become a problem as a company grows. Whenever a new user comes, his or her credentials need to be recorded individually sometimes in different databases for each service accessed. In addition, when users leave the company, the inverse process needs to be done in order to ensure that no security breaches are left in the network.

Kizza (2005) referred to the previous issue indicating that "one of the system administrator's biggest problems, which can soon turn into a nightmare if it is not well handled, is controlling access of who gets in and of the system and who uses what resources, when, and in what amount" (p. 209); in spite of this, Bhaiji (2008) stated that "network access control is one of the most important measures that is often overlooked" (p. 267).

The use of Authentication Authorization and Accounting (AAA) protocols can provide a solution to many concerns that the network administrator face in the area of access control and network security. AAA protocols can provide in its own way three of the five basic network security functional elements established by Fung (2005): (a) authentication, which provides basic access to the network by identifying legitimate users; (b) authorization, which controls access to network resources based on user's profile and permissions; and (c) non-repudiation by mean of accounting or auditing the user's actions.

The main focus in this area will be given to users' authentication by means of Network Access Servers (NAS) that interacts with an AAA server to handle authentications. Currently there are three AAA protocols that can be used to implement such solution: DIAMETER, TACACS+ and RADIUS.

DIAMETER is a relatively new protocol that is not supported by many devices. TACACS+ on the other hand is a proprietary protocol developed by Cisco, due to its nature is not an alternative to be used when dealing with devices from different vendors. RADIUS is an open protocol that can be used as an alternative to TACACS+.

The main benefit of RADIUS is that it grants flexibility and interoperability between different vendors, since it is an open protocol available without restrictions for particular implementations; this implies that vendors can include particular characteristics in their products and still keep the basis to make it operable with products from other manufacturer. Bhaiji (2008) stated this as follow:

> One of the main objectives of the RADIUS protocol standard is to provide interoperability and flexibility between RADIUS-based products from different vendors. For this reason, RADIUS is a fully open standard protocol, distributed in C source code format, and can be used unrestrictedly by any vendor or customer. This allows for the flexibility of being able to modify RADIUS to work with any security system currently available on the market. (p. 270)

Thanks to this, low cost solutions in open source format are available for implementation, particularly in the form of a FreeRADIUS server. The final security concept that the new network topology will address is the use of centralized authentication systems, using the RADIUS protocol.

Wireless networks.

Wireless technologies have become more available in recent years and have been the subject of several innovations that have increased the transmission speed and the different services provided by these. Dekleva, Shim, Varshney and Knoerzer (2007) presented a concise record of the wireless services evolution from 1970, when these were limited and expensive, to the present days, when service applications range from personal entertainment and multimedia to business oriented and positioning systems.

Due to the many wireless technologies currently in use, when talking about wireless networks, it becomes necessary to make a differentiation between the different types of wireless networks in existence. Wilton and Charity (2008, p.38) made a division of the wireless network systems between cellular networks such as GSM, which were originally devices for voice coverage, but can also be used as Wireless WAN, and the IEEE 802.11 Networks, which were born as an alternative to the Ethernet technologies. Geier (2010, p. 26-34) made a mention of technologies such as WiMAX, used for Wireless MANs, Bluetooth, and Zigbee technologies. Under the context of this research, wireless networks will be understood as WLANs using the 802.11 standards.

802.11 Technologies are closely related to the Wi-Fi alliance, which tests interoperability between 802.11 products. Geier (2010) defined the Wi-Fi alliance as "an international, nonprofit organization focusing on the manufacturing, marketing and interoperability of 802.11 WLAN products" (p.24). The standards have evolved through the years, increasing the transmission speed and providing compatibility with some legacy standards. The most recent standard is 802.11n, compatible with the previous 802.11g and 802.11a, approved in 2009 and capable of operating at frequencies of 2.4 GHz and 5 GHz.

Bhaiji (2008, p. 349) presented four basic components of a WLAN network:

1. Wireless Access Point (WAP or AP): Is a device (hardware or software based) that connects the different wireless communication devices and relays data between the wireless and wired network.
2. Wireless Network Card (NIC): Is a component needed by any device that needs to access the wireless network. It scans the area and associates the device to an AP.

3. Wireless Bridge: Are optional devices that are used to connect multiple wired or wireless LANs at the data link layer, they are capable of covering longer distances than APs so they are particularly useful in building to building interconnections.
4. Antenna: It radiates the wireless signal through the air in order for clients and APs to send and receive transmission. Antennas can determine the range and the propagation characteristics of a wireless device depending on their shape and type.

Cisco Systems et al (2004, p. 234) presented a different classification of components, dividing them in two types: The wireless client, is the basic component of the WLAN, and needs to be present in order to build a wireless network; and the AP, which acts as bridge between the wireless and wired networks. Depending on the physical architecture of WLAN that is being configured an AP might not be necessary, just like in the case of Ad Hoc WLANs.

WLANs physical architectures.

Geiger (2010, p. 55-62) defined three types of physical architectures for WLANs: Ad Hoc, Infrastructure, and Mesh. Characteristics of each of these architectures are presented below.

An Ad Hoc network, also known as independent basic service (IBSS) is a basic architecture that requires little pre-configuration; being particularly useful in a medium where a WLAN with AP is not available, since multiple clients can be interconnected as long as they are within radio range and the IBSS parameters are properly configured.

Infrastructure WLANs are the most commonly used by companies and homeowners; they make use of AP to connect clients to the network. Each AP is

connected to the wired network and connects the users by forming a radio cell, called basic service set (BSS) any user within the BSS can connect to the AP. If BSS are set up to overlap with one another, users can roam through the different BSS without losing connectivity, this is called roaming.

Mesh networks, as their name implies, make use of mesh nodes, which are very similar to AP but are connected to each other wirelessly, avoiding the need of Ethernet connections between them. Mesh networks are particularly useful in places where wiring is not feasible. Client's connection is similar to the one used in infrastructure WLANs, with the difference being on the mesh node, which implements a proprietary routing protocol which routes packages until they reach their destination.

Securing wireless networks.

One issue of significant importance when implementing wireless networks comes in the security vulnerabilities that it might arise. Geier (2010, p.87) presented three areas where security vulnerabilities might arise when implementing WLANs: Passive monitoring, unauthorized access and denial of service.

Passive monitoring can easily occur in wireless networks since their scope usually can go beyond the physical boundaries of a company. An individual can use a sniffer to capture all the traffic flowing through the network and obtain sensitive data. This issue can be solved by the implementation of encryption mechanisms in the WLAN.

Wired Equivalent Privacy (WEP), and Wi-Fi Protected Access (WPA) are common encryption methods used to secure WLANS. Bhaiji (2008, p. 350) ties authentication and encryption as the two main components of WLAN security; although WEP and WPA provide a basic form of authentication, the implementation of the

802.11x standard combined with Extensive Authentication Protocol (EAP) might be used to provide identity based network access control. This can be implemented by means of AAA protocols working together with the APs.

Unauthorized access occurs when someone gains access to the organization's network, including services and applications. WLANs are more vulnerable to unauthorized access, particularly if there are no encryption mechanisms implemented. Bhaiji (2008, p. 351-352) indicated that a simple way to prevent unauthorized access, apart from encryption is by disabling service set identifier (SSID) broadcasting; which might prevent someone from accidentally accessing the network, but does not provide complete protection from unauthorized access, therefore, it has to be accompanied with other security mechanisms. Since the SSID is the name of the wireless network which is usually broadcasted by an AP in plain text, if a client does not know the SSID he/she will not be able to access the network.

Denial-of-Service (DoS) occurs when an attacker renders the WLAN unable to work. Geier (2010, p.95) indicated that even when using modern security mechanisms, wireless networks are extremely vulnerable to this type of attacks. By using a "brute-force" method of denial of service a WLAN can become ineffective in two ways: Either by a massive flood of packets that forces the network to shut down, or by using strong radio signals that might render NICs and APs useless.

The telecommunication laboratory equipment permits the development of wireless practices related to the implementation of WLANs under infrastructure architecture and some practical implementation of security mechanisms for wireless networks. The laboratory practices cover topics such as the different WLAN standards, the use of

encryption mechanisms to avoid passive monitoring, as well as authorization mechanisms to avoid unauthorized access.

Network convergence.

It was already discussed early in this chapter how network convergence has become a trend widely adopted by companies, allowing the integration of services in the existing computer network infrastructure. Network convergence also reduces the complexity of services infrastructure, as companies grow and service requirements increase, the integration of IT and communication services, not only reduces costs but the management load as well, Bhaiji (2008) defined this situation as follow:

> At the same time networks are growing exponentially, they are becoming complex and mission critical, bringing new challenges to those who run and manage them. The need for integrated network infrastructure comprising voice, video and data (all-in-one) services is evident... (p. 5)

Macaulay (2006, p.12-14) presented a general view of the convergence market, starting from VoIP, which is the technology with the earliest impact and significance; and covering technologies such as IPTV and the Triple Play phenomenon; Digital Video Surveillance and the integration of CCTV in the data network; management of PLCs in industrial environments among others.

Each of these technologies can be further explored, but this study is focused on the implementation of VoIP. Contrary to wireless networks, the importance of VoIP comes mostly from a business standpoint. Hens and Caballero (2008, p.32) indicated that VoIP alone might not bring anything new to subscribers –or regular users, in the case of a company. –since they don't notice the migration from the public switched telephone

network (PSTN) to IP transport infrastructures, while this is might prove true from the standpoint of a service provider in relation to a home subscriber, Cioara, Cavanaugh and Krake (2009, p. 34) indicated that from a business standpoint, where VoIP is implemented to manage the internal telephony services, the benefits include but are not limited to:

1. Reducing the cost of communication, since instead of tie lines or toll charges to communicate between branches, the call can be forwarded over a WAN connection.
2. Cabling cost is reduced, due to the fact that the voice network is integrated in the data network.
3. Seamless voice networks, because the voice network inherits the properties of the data network, the voice traffic travels through the network rather than exiting to the PSTN, providing centralized control of the voice devices attached to the network and a consistent dial plan.
4. Unify e-mail, voice mail and fax, as well as the addition of extra benefits to phone calls.

From a technical standpoint, Hens and Caballero (2008) indicated that "the main advantage of IP telephony is that it enables the convergence of data and voice. But convergence is not possible without QoS aware networks" (p. 32). Davidson, Peters, Bhatia, Kalidindi and Mukherjee (2006, p. 121) indicated that among the issues that VoIP technology faces, QoS can help solve:

1. Packet Loss: A common situation in data networks, particularly over a high flow of traffic.

2. Jitter: The variation of the arrival time of voice packets, meaning that packages not arrive at a regular interval but might experience a difference between the difference arrival times.
3. Handling delay: The delay produced by the different devices that forward the voice frames through a network.

Davidson et al (2006, p. 120), also indicated that in order to achieve the best QoS it is important to separate functions occurring in the edge and backbone of a network.

Implementing a VoIP infrastructure.

Cioara et al (2009, p. 34) stated that before achieving VoIP service in a company, the proper foundational infrastructure of the network must be established beforehand. This includes technologies such as Power over Ethernet (PoE), VLANs, and DHCP services.

PoE allows the powering of devices by means of an Ethernet cable connecting the device and the Ethernet switch; it could be argued that power can be supplied in a different way, but PoE allows for a centralized point of power distribution and permits devices that are not located near a power outlet to be powered in this matter. The 802.3af standard defines the way that PoE works: A small DC current that does not affect the performance of non PoE devices is used on the switch with PoE capability to detect when a PoE device that needs to be powered is connected, this device has a resistor that returns an specific level of resistance to the line and in this way the switch determines how much power it has to send to the attached device.

The second technology needed for the foundational infrastructure of a VoIP network is VLAN. Thomas II et al (2001, p. 172) defined VLAN as "a Layer-2 logical

network that enables the network administrator to connect network devices, even if they are physically dispersed. Each VLAN functions as a separate broadcast domain". VLANs' importance in relation to VoIP comes from the fact that it's a recommended practice to separate voice and data traffic in a network, Cioara et al (2009) referred to this situation as follow:

> Separating voice and data traffic using VLANs provides a solid security boundary, keeping data applications from reaching the voice traffic. It also gives you a simpler method to deploy QoS, prioritizing the voice traffic over the data. (p. 73)

In order to allow a PC and an IP phone to be connected to the same switchport, VLAN tagging becomes necessary; this is achieved by means of the 802.1Q protocol. Indirectly this also limits the use of VoIP to switches with 802.1Q capability.

DHCP is the final technology needed to properly build a VoIP infrastructure; DHCP dynamically assigns an IP address to the IP phone based on the address pool set up for the VoIP VLAN. DHCP can be achieved by means of an independent DHCP server or by the use of the router in-built DHCP server.

The equipment available in the telecommunication laboratory permits the development of an introductory laboratory practice in the area of converged networks that provides application examples of the technologies required in a basic implementation of a VoIP infrastructure, including VLANs, PoE and DHCP.

Chapter 3

Design Methodology

This chapter explores details related to the methodology that was followed to design and deploy the new laboratory topology starting from the original topology and its elements and then dividing the deployment in different phases covering practices that share common points.

Deployment Considerations

During the design of the topology and practices it was necessary to consider that one of the primary objectives of the study was to improve the use of resources in the existing telecommunication laboratory topology by improving the utilization of the equipment currently available. The laboratory practices not only intend to improve the students' comprehension of the concepts in the areas previously presented but seek to build a topology that improves the use of the existing equipment. Since these practices are not intended for an introductory course in computer networks, the student are presented with a starting network layout that already has full connectivity; Figure 1 presents the initial configuration of the network. From the starting network, the new topology is implemented by the development of the laboratory procedures.

The network equipments presented in the basic laboratory network are listed below:

1. Computers acting as hosts, in the access layer of the network.
2. Hubs, interconnecting devices in the access layer.
3. Cisco 2500 Series routers, on the distribution layer.

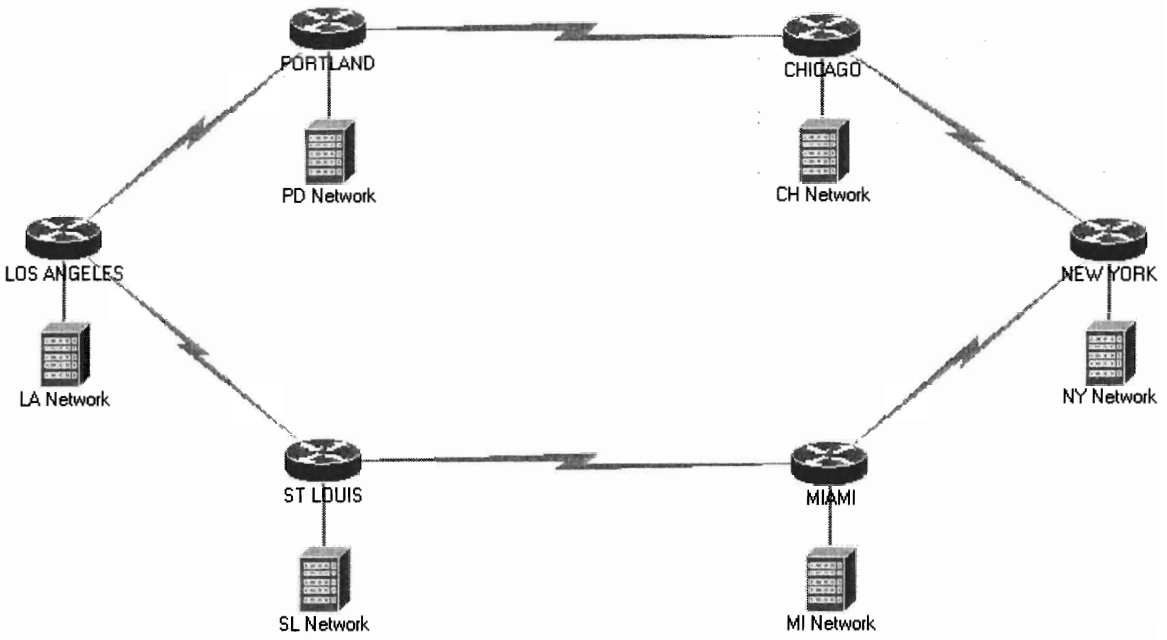


Figure 1. Starting laboratory network layout. The six routers are interconnected between them by a serial link. Buildings represent one or more hosts belonging to a router's network, connected by an UTP cable through a hub.

Using hierarchical design principles it can be established that the major point of concern for the student will be in the distribution layer. Thomas II et al (2001, p. 87) indicated that this layer deals with policies for access and connectivity, encryption, QoS, among other things; which remarks its importance in the scheme of advanced topics in data communications, particularly in the subdivisions of security and traffic management in regarding access and security policies.

The basic network consists of six different branches of a hypothetical company which are interconnected by serial links forming a ring. It can be assumed that users inside the different branches either don't have access to the Internet or the access is

managed locally and outside of the corporate network, which might lead to a security breach in terms of unauthorized access to sensitive information.

During the development of the laboratory practices, the students take the role of a newly hired network administrators with the task of implementing security solutions and different services to the company network. Practices have been grouped in deployment phases related to the status of the whole network and the integration of services and features. By developing the practices in an orderly manner and completing the different deployment phases the following devices are integrated in the starting topology:

1. Computer Servers, providing different services to the network
2. Cisco 2800 Series Routers, working as access points for Wireless Networks and providing VoIP services.
3. Switch to provide interconnections for different devices.
4. Cisco PIX firewalls.

Deployment Phase 1: Secure Internet Access

One of the earliest problems the students will face as network administrators will be the integration of Internet access for all the branches in a corporate network with a single network perimeter or exit point. By doing this, the implementation of future practices in areas such as network monitoring or traffic control becomes much easier since a point where the traffic of the different networks comes together is defined.

The newly created network perimeter must be secured to protect the internal network from the outside network, while at the same time ensuring the communication between them and ensuring that network services will be provided for both sides as needed. The first deployment phase provides a solution to the previously presented

situation; it is mainly focused in the area of network security, and provides students with a better understanding of the following concepts:

1. Firewalls and their role in a secure network model.
2. ACLs.
3. Perimeter Networks/ DMZs.

A single laboratory practice, labeled as Practice #1, covers all these areas; students work with two PIX firewalls and the different hosts located in the intranet, DMZ and external network, in order to verify connectivity. By completing laboratory Practice #1 the student are expected to:

1. Configure the necessary parameters on PIX firewalls to set up a basic DMZ layout.
2. Configure Access Control Lists (ACLs) based on communication protocols.
3. Perform basic troubleshooting of communication issues between segments of a network.

A general scheme of the network after the procedure has been implemented is presented in Figure 2. Continuing with the case of a hypothetical company, it can be observed that the network architecture has increased its complexity with the addition of firewalls that divide the network in three parts: A segment for the internal network, consisting of the original network; a segment for the DMZ, hosting the servers; and the external network (Internet).

In order to facilitate implementation, some considerations have been established: Both the Linux and Windows servers in the DMZ can be used to provide the network with all the services it needs, implying that they might be accessible to users in a

potential extranet and the Internet in accordance to the company security policies and the laboratory needs. The perimeter firewall that connects to the external network provides network address translation to the hosts in the internal network.

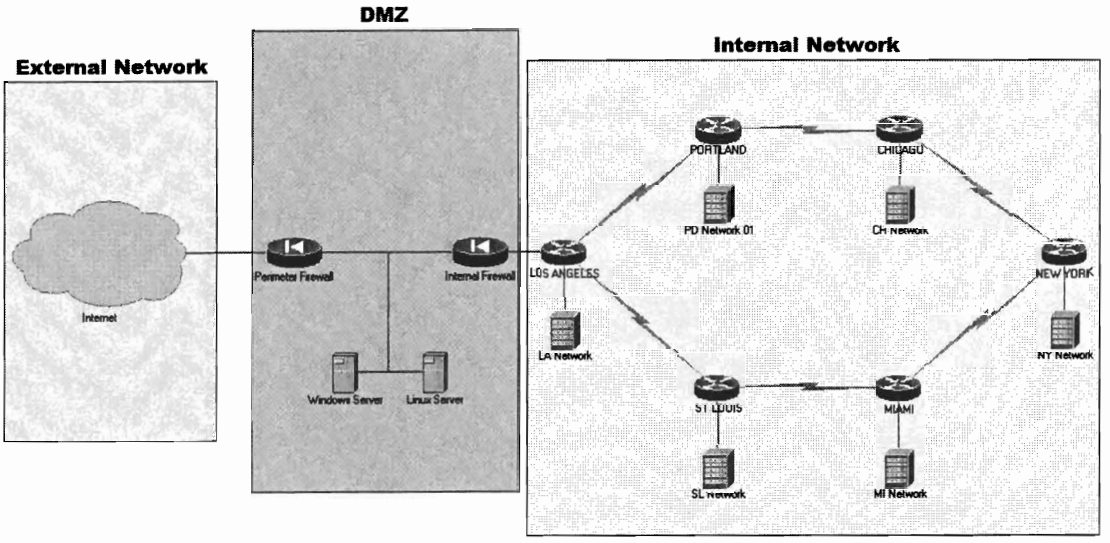


Figure 2. Network layout after implementing a secure perimeter for Internet access. The laboratory network is effectively divided in three segments: The internal network, the DMZ and the external network representing the Internet.

Deployment Phase 2: Connecting Remote Sites by VPN

The second deployment phase involves the incorporation of two Cisco 2800 series routers in the laboratory infrastructure. Continuing with the role as network administrators, after the students have established a perimeter for secure access to an external network, they are presented with a second issue: New branches of the company are established in remote locations; and the cost of inverting in a dedicated WAN serial link cannot be afforded. Students, as are entrusted with the task of connecting the new branches to the corporate network by means of a site-to-site Intranet VPN. The second

implementation phase covers the implementation of a VPN tunnel between the new locations and the corporate network. It provides the student with application examples of the following concepts in the area of network security:

1. Network Address Translation (NAT).
2. Port Address Translation (PAT).
3. Virtual Private Networks (VPN).
4. IPSec

This phase comprises two laboratory practices: Practice #2 and Practice #3. Practice #2 covers both NAT and PAT implementation. The Cisco 2800 series routers and the PIX perimeter firewall are used by the students to perform the following tasks:

1. Define groups of hosts that will participate in the NAT process.
2. Establish a pool of addresses for NAT purposes.
3. Configure NAT in routers and firewalls.
4. Configure PAT in routers and firewalls.
5. Troubleshoot and verify typical NAT and PAT configuration.

Practice #3 covers the last two points of the second phase, while presenting content that has already been reviewed by the student in previous practices. This practice focuses on establishing a VPN link between three sites and presents a practical example of device interoperability. The Cisco 2800 series routers and PIX perimeter firewall are used by students in order to accomplish the following objectives:

1. Configure the basic parameters for the establishment of a security association (SA) between different sites for VPN purposes by means of Internet Protocol Security (IPsec).

2. Configure Internet Security Association by using Internet Key Exchange (IKE) and Key Management Protocol (ISAKMP) policies for encryption and authentication.
3. Configure data connection parameters for VPN, including transform sets and crypto-maps.

The physical topology of the telecommunication laboratory doesn't experience any changes after this phase has been completed. The subsequent practices deal with the implementation of different services and security features under this physical topology. Figure 3 presents the network scheme after the successful development of this phase.

Deployment Phase 3: Implementing a VoIP and Wireless Infrastructure

At this point, students within the remote branches have access to services that were originally only available to the internal network but services such as VoIP and WLAN are not available. The third phase is concerned with the implementation of these services in the laboratory. The Cisco 2800 series routers are devices designed to offer integrated services of Wireless, VoIP and security features for small to large offices and provide a basic understanding about the deployment of this solutions with self management. A basic implementation of both VoIP and Wireless infrastructure set the stage for the development of more advanced laboratory practices in the areas of QoS and security management. The students are assigned with the task of deploying a WLAN and providing services of VoIP in small branches of a company. The purpose of this stage is to provide students with practical knowledge in the following areas:

1. VLANs
2. VoIP implementation

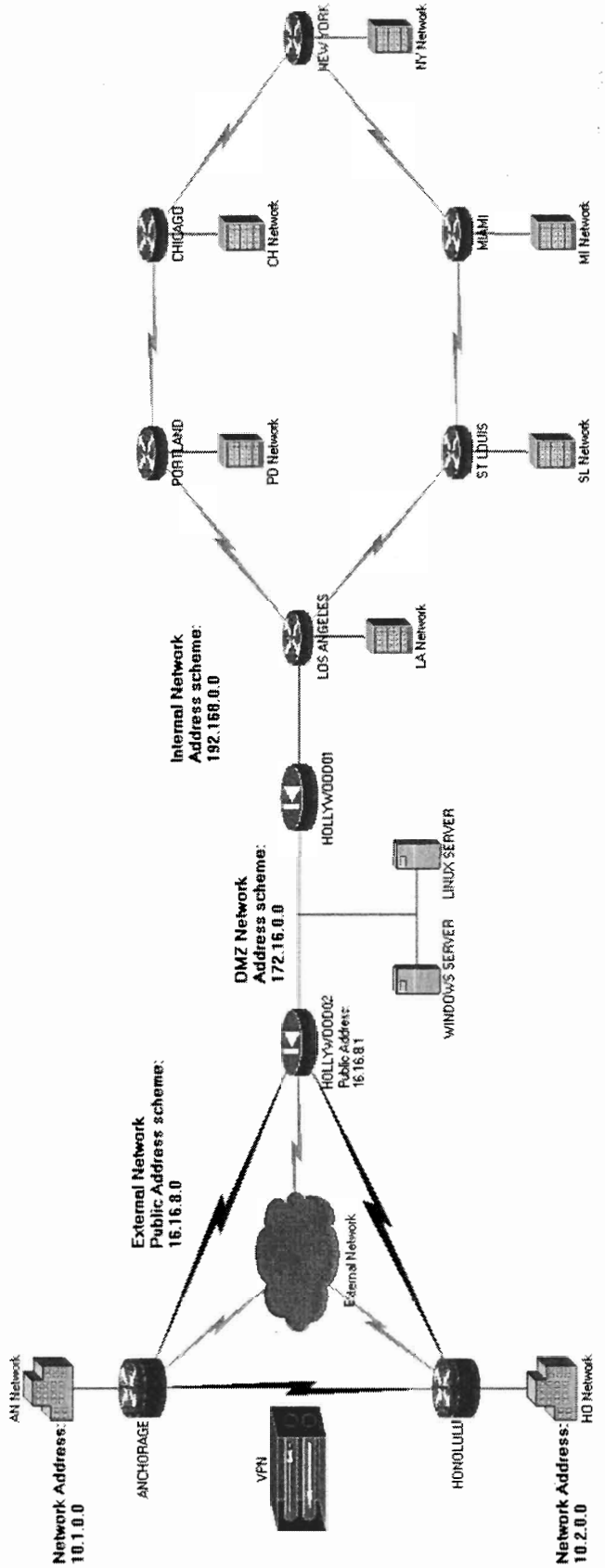


Figure 3. Network layout with multiple VPN connections. At this point all the equipment in the telecommunication lab has been incorporated in the network and no more changes are done to the physical topology.

3. Wireless networking standards.
4. Wireless configuration.
5. Basic wireless authentication.

The third phase consists of two laboratory practices: Practice #4, introduces the concept of converged network and provides basic configuration guidelines for VoIP; Practice #5, provides basic knowledge related to WLANs, how to implement them and how they work.

Practice #4 introduces IP phones, QoS and VLAN configuration, as part of the required elements for the deployment of VoIP. Usually, a switch with VLAN capabilities might be required for the deployment of a VoIP solution; nevertheless, the Cisco 2800 router includes an interface which can be configured as a switch. The student will perform the following tasks:

1. Configure virtual local area networks (VLANs) for data traffic and voice.
2. Configure quality of service (QoS) parameters to be used in Voice over IP (VoIP).
3. Configure dynamic host configuration protocol (DHCP) services in the router.
4. Configure ports in a switch for VoIP.
5. Configure IP phones features.
6. Verify communication between VoIP devices.

Practice #5 takes the Cisco 2800 router as wireless Access Point (AP) by means of the HWIC wireless interface, during the course of the practice the students will perform the following tasks:

1. Configure the basic settings of an infrastructure Wireless Local Area Network (WLAN)

2. Define the Service Set Identifiers of a WLAN and their behavior.
3. Perform the basic configuration of radio channels and define the behavior of the antennas.
4. Configure basic security features for infrastructure WLANs.

Deployment Phase 4: Remote Users Access through VPN

This phase covers concepts in the area of remote-access VPN, providing a review of the concepts previously examined in the previous VPN practice, including IPSec, IKE, ISAKMP and SA among others. The students have the task of connecting remote users using a VPN client, to the corporate network. By the end of phase 4, the students will have obtained some practical insight in the following areas of network security:

1. Remote-access VPN configuration.
2. Local user authentication.
3. IKE Mode configuration

A single laboratory practice named Practice #6 covers all the aspects of phase 4. The PIX firewall working as a perimeter firewall for the main corporate network will be used for the development of this practice, which requires the students to perform the following tasks:

1. Set up the configuration in the host and PIX to allow a remote-access VPN connection to the network.
2. Configure an IP address pool for the remote clients.
3. Set up the authentication settings in the PIX, including usernames and passwords for remote clients.
4. Establish a security association between a remote client and the PIX.

Despite consisting of a single laboratory practice and being closely related to the VPN area, it was decided to separate this section from phase 2 since by completing this phase and implementing a wireless infrastructure network, which is the last practice of phase 3, the students set the basis for the last deployment phase. Concepts related to authentication are further covered in phase 5.

Deployment Phase 5: Centralized Authentication

This phase address the issue of centralizing both wireless and VPN authentication in order to improve the management of a network that experiences growth in terms of users. As stated in the previous chapter, when the company grows, the number of users that require access to services such as WLAN, remote access to the corporate network, among other things, increases as well and leads to a situation in which managing independent devices with distributed user's authentication information becomes a problem for the network administrator. Phase 5 provides some insight in this issue and some practical examples of centralized authentication by means of AAA protocols. During the development of this phase the student will acquire first hand experience in the following areas:

1. AAA protocols.
2. Radius protocol.
3. Centralized Authentication.

This section is covered in two laboratory practices: Practice #7 introduces the students to the AAA protocols and the RADIUS server; Practice #8 introduces the student to the process of centralizing authentication for WLAN and remote users that access the networks through VPN.

Practice #7 intends to familiarize students with the client-server model used by the AAA protocols, by means of exploring and modifying the settings of a Linux Server running FreeRADIUS, this practice allow the students to:

1. Understand the general operation of AAA protocols and a RADIUS server.
2. Initiate a RADIUS server in debug mode.
3. Access users and NAS databases and identify their fields.
4. Introduce user and NAS information for future authentication.
5. Verify the correct operation of a RADIUS server.

Practice #8 focuses on the modification of the previously defined users' authentication scheme for both the wireless networks and the remote-access VPN. This practice covers two subjects due to the similarity of the implementation in both cases. By completing this practice the students will see some practical examples regarding the use of the RADIUS server by performing the following tasks:

1. Establish parameters for communication between the Wireless AP, the firewall and the RADIUS server.
2. Configure centralized authentication for wireless and remote-access users.
3. Verify and troubleshoot user authentication in the WLAN and the VPN.

By completing the laboratory procedures in this phase the network will have reached its objective in terms of students learning, and will present the possibility for development in other areas such as accounting of services and other security principles that could be addressed in future research.

Chapter 4

Development and Evaluation of Laboratory Practices

This chapter provides details regarding the development and evaluation of the laboratory practices previously described. All practices consists of two sections: A guide presenting a theoretical basis and describing all the procedures to follow in order to accomplish the objectives; and an activity review sheet, containing several activities that require the students to provide some answers. The activity review sheets were developed in ways that allow both the instructor and the student to identify if there are problems during the process of completing the guide. The laboratory guides were divided in the following sections:

1. Objectives of the practice: This section is defined in a way that allow both the instructor and the students to easily identify when key activities are properly finished and the objectives are accomplished.
2. Introduction of the problem: This section presents a scenario that shares similarities with real life situations that a company might experience.
3. Theoretical background: This section is usually identified as *Part I* (With the exception of Practice #6 and Practice #8) and provides a basis for the concepts covered in the practice. It is important to consider that the practices are not a substitute for the theoretical foundations that might be defined during a lecture but intend to enforce these concepts by providing examples of their applications.
4. Interrelated activities: Consisting on several sections identified as *Parts* with subsequent Roman numerals, consisting of activities that might generate an identifiable output after being performed.

The activity review sheets were divided in parts identified with alphabetically ordered capital letters that correspond to the Roman numbered parts of the laboratory guide. The review sheets were designed to be implemented together with the laboratory guides: Starting from the end of the first Roman numbered part of the laboratory guide, the students are asked to perform a set of activities presented in the first alphabetically numbered part of the activity review sheet; after completing the section, the student are indicated to continue with the next section of the laboratory guide.

Most of the laboratory practices, with the exception of the last two practices were evaluated by at least two students. The students selected to perform these evaluations were selected from groups of both graduate and undergraduate students that either had some previous background in computers networks or were taking a course related to data communications.

The evaluations of the laboratory practices were performed with the use of two types of evaluation sheets: One for each of the students participating in order to determine the following facts: (a) The accomplishment of the objectives listed in the practices; (b)student comprehension of objectives and procedures; (c)clarity of instructions and figures; and (d) students impression of the practice, including how likely would the student recommend the use of the practice and any suggestion regarding it. The instructor coordinating the practice used an evaluation sheet to record information like: the time taken by the students to complete the laboratory practice, the assistance provided during the process and any additional information. The overall format of the evaluation sheets can be found in Appendix B while the evaluation results are detailed in Appendix C. A typical evaluation process for a laboratory practice consisted of the following steps:

1. The students participating in the laboratory practice evaluation process were provided with the practice guidelines and with an evaluation sheet. The students were instructed to read the guidelines before starting the practice.
2. The students proceeded to perform the laboratory practice in accordance to the guidelines defined by the instructor and the guide. The starting times of the practices were recorded by the instructor in his evaluation sheet.
3. The student performed the indicated procedures and tasks needed to complete the practice. Meanwhile, the instructor recorded data regarding the assistance provided to the students as well as any significant observation.
4. After completing the practice, the instructor recorded individual completion times and the students were asked to complete the review sheets.
5. The review and evaluation sheets were collected by the instructors while the students were allowed to keep the laboratory guide.

The evaluations of the laboratory practices allowed the identification of issues related to spelling, typos, instructions, and student comprehension among other things. Laboratory practices were subject to modification and improvement based on the feedback of the students. The following sections provide further details regarding the process of developing each practice as well as several results obtained from the evaluation.

Laboratory Practice #1

The title of the practice is "Implementing a Demilitarized Zone (DMZ)". This practice provides an introduction to PIX firewalls configuration, including basic instructions and formats. Practice #1 also includes an application example of ACLs,

particularly extended ACLs that restrict protocols, as well as a basic introduction regarding the design of network architectures. This practice can be incorporated in either a network security course or a networking course that covers the area of ACLs in either graduate or undergraduate level. For the development of this practice it was necessary to set up different network services that were to be allowed or restricted based on access policies. These services were implemented by means of a computer working with the OpenSUSE 11.3 Linux operative system and acting as a multipurpose server for the laboratory network. The services implemented for the network clients were: DHCP, DNS, FTP and Web.

Other issue presented during the development of the practice was related to routing within the DMZ. Depending on the PIX routing configuration, elements located within the DMZ were able to communicate with one segment of the topology (external network or internal network) but not with the other segment. This problem was solved by configuring the Linux server as a static router for the DMZ. Appendix D presents all the configuration details regarding the Linux server.

The practice was evaluated by a group of four undergraduate students that at the moment were taking an advanced course in the area of routing and switching. From the instructor evaluation sheet it was concluded that the average completion time of the practice was 1 hour and 15 minutes, with all students finishing simultaneously. The instructor was asked for assistance (6 times) regarding the following issues:

1. Physical location of the devices that were being configured.
2. Methodology of the laboratory practice. Particularly regarding how to complete the activity review sheet.

3. Names of firewall's interfaces in relation to a task presented in the activity review sheet.
4. Information regarding networks directly connected to the firewalls.
5. Access to the web server after completing a section of the laboratory guide.

Most of the issues indicated by the students were in relation to the activity review sheet, a latter faculty revision of the laboratory practice proved this issues and the activity review sheet was revised and modified in order to improve the clarity of the guidelines.

Student's evaluations of Practice #1 were positive with a modal score of 5 and a lowest score of 4 in a 5 points scale for all of the items presented in the evaluation sheet. The only significant suggestion was the use of the Mozilla Firefox web browser over Microsoft Internet Explorer in order to improve the navigation.

Laboratory Practice #2

The second laboratory practice is called "Network and Port Address Translation (NAT & PAT)". This practice introduces the students to the Cisco 2800 series routers presenting basic commands such as the definition of an IP address for the interfaces. This practice works well as a standalone introductory practice for a network security course aimed to students with some background in computer networking, since it covers some basic commands that can be taken as a review. Issues regarding the development of this practice were mostly related to a particularity of the Cisco 2800 routers that possess an integrated switch module with several interfaces that have to be set up in a way that resembles a switch. The interface that works as a gateway for the equipment connected to this integrated switch is by default the VLAN 1 interface. In the original implementation of the practice, interface VLAN 1 was used as the NAT inside interface, later this had to

be modified in order to avoid conflicts with other VLAN implementations. The use of an interface other than VLAN 1 for data transmission required the incorporation of the new VLAN in the switchport configuration which extended the length of the practice. Even though the practice doesn't address the concepts of VLANs in deep, it was necessary to provide some insight for the student.

In addition to the Cisco 2800 series routers this practice also uses the perimeter PIX firewall from Practice #1. Before the implementation of Practice #2 by the students, is necessary for the instructor needs to erase the NAT and PAT configuration in the PIX firewall and introduce a basic configuration for the Cisco 2800 series routers, which includes hostname, password and static routes. Further details regarding the preliminary steps for the implementation of the different practices are presented in Appendix E.

Practice #2 was developed by a group of five graduate students taking the Network Security course and was the first practice to be evaluated by students. The original implementation of this practice didn't have an activity review sheet which reduced the time of implementation to an average of 30 minutes, however, this affected the troubleshooting process as well as student's comprehension, which led to the conclusion that it was necessary to add a review sheet to future evaluations in order to obtain better comprehension and avoid troubleshooting issues by the end of the practice. Assistance from the instructors was reasonably required (5 times) in the following areas:

1. Terms definitions and theoretical explanations.
2. Command syntax issues.
3. Troubleshooting at the end of the practice.

Overall, the student evaluation was positive for most of the areas, with an average score of 4.16 in a 5 points scale, the modal evaluation score was of 4 and the lowest was 3. Low scores were given to the areas of theoretical explanation and the usefulness of figures, indicating that the network diagram needed to be improved as well as the definition of concepts.

Laboratory Practice #3

The third laboratory practice is titled "Virtual Private Networks (VPN)" and intends to provide some insight in the area of VPN implementation by means of IPSec. Practice #3 would work better in a network security course as a practical application example of the IPSec protocol suite, encryption and authentication mechanisms but can be implemented at the end of an advanced course in computers networks that covers concepts such as ACLs and NAT. Issues regarding the development of this practice were mostly related to interoperability between firewalls and routers and the identification of common points during the configuration in order to arrange the guide in a way that highlights the similarities of the procedures.

Deal(2002, p. 474-487) provided an explanation of the process of configuring an IPSec VPN for a site to site connection but this process was limited to PIX firewalls establishing a connection for two sites. Bhaiji (2008, 445-454) on the other hand, provided some configuration examples IPSec VPN tunnels in a router to router scenario. The procedures presented by these authors had to be adapted to the telecommunication laboratory situation in order to allow a multiple site-to-site connection using different types of devices.

The laboratory practice was evaluated by a group of three undergraduate students involved in an advanced course of routing and switching. It was established from the instructor evaluation that the average time for completion of this practice was 45 minutes. Instructor assistance was required (6 times) in the following areas:

1. Procedures and theoretical concepts explanation.
2. Troubleshooting regarding connectivity.
3. Configuration problems regarding transform sets.

Some of the questions presented in the activity review sheet needed to be modified and some procedures were improperly presented which caused some comprehension problems. Another issue presented was the need for close observation from the instructor in order to avoid mistakes regarding command typing and procedures. Despite the complexity of the procedures, the evaluation was positive with a 5 modal score in a 5 points scale with the lowest score being 4 in regards to the usefulness of the diagram. Based on the instructor's observations and the students' suggestions it was necessary to provide a further insight in the area of security mechanisms and IPSec because the students needed some additional background in the area of network security. This indicates that the best scenario to implement this practice is under a network security course.

Laboratory Practice #4

The title of the fourth laboratory practice is "Implementation of Voice over IP (VoIP)". Practice #4 provides a practical example of network convergence in the form of VoIP and might be implemented at the end of an advance course in networking for either undergraduate or graduate students in order to provide some insight in the topics of

Converged networks and VoIP. A special topics course may be needed in this area which might lead to the creation of more practices covering VoIP concepts, although the lack of equipment might present a problem for large groups of students. Another possibility might come in the form of a course presenting different technological applications of computer networks that introduces the student to several areas of interest in telecommunications.

No particular issues were noticed during the development of this practice. The problems presented came mainly from the actual implementation of the procedures. The Cisco IP phones and the routers generate configuration files that have to be deleted by the instructor prior to a new implementation of the practice. Additional details regarding how the instructor has to address this issue are presented in Appendix E.

The laboratory practice was evaluated by two graduate students enrolled in a networking course and with previous experience and coursework in computer networking. The average completion time was established to be 1 hour and 13 minutes. Instructor assistance (6 times) was required in the following areas:

1. Transition between laboratory guide and review sheet.
2. Output from the router and troubleshooting.
3. Correction of procedures in the guide.

This laboratory guide underwent several corrections and modifications to avoid conflict with previous procedures implemented in the laboratory equipment. The student evaluation was overall positive with an average score of 4.5 in a 5 points scale. The lowest score was 3 and it was associated with the visual help provided in the guide. Scores of 4 in the area of theoretical explanation indicated a need to further clarify the

concepts although they might be associated with the fact that the students were being introduced to them without previous coursework in the form of lectures.

Laboratory Practice #5

The fifth laboratory practice is titled "802.11 Wireless Local Area Networks". This practice introduces several concepts in the area of mobile communication and provides a practical example of infrastructure WLAN implementation. This practice can be implemented as part of an undergraduate or graduate course in special topics in the area of wireless networks or as part of a network security course that covers the area of wireless networks security.Two wireless NICs were acquired to be used together with the Cisco 2800 Series routers for the proper development of Practice #5. The main issue presented during the development of this laboratory practice is related to the association of WLANs with the different wireless networks and the use of multiples subinterfaces in a single radio interface: If the parameters are not properly assigned, the wireless clients will be able to access the network but won't be able to receive their DHCP parameters nor access their gateways.

Practice #5 was evaluated by a group of four undergraduate students in the course of Advanced Routing and Switching. The average time the students needed to complete the practice was 50 minutes. During the course of the evaluation the instructor assistance (5 times) was required in the following areas:

1. Corrections to the review sheet and guidelines.
2. Routers reloading.
3. Authentication issues.

One of the routers had to be reloaded due to conflicts with some VLAN parameters that had been set up prior to the practice. Other problems related to password and authentication parameters, as well as some mistakes in the guidelines were addressed during the evaluation and corrected later. Overall, the students' evaluation was positive with a modal score of 5 in a five points scale for most of the items. The lowest score was 4 in the area of clarity of procedures given by two students, theoretical explanations were also indicated as an area that could be improved. Recommendations from the students include the development of methods to have the students take some time to review the procedures.

Laboratory Practice #6

Practice #6 is titled "Remote-Access VPN". This practice reviews some of the concepts presented in Practice #3 and provides an example of the implementation of remote-access VPN. Since Practice #3 introduced most of the concepts related to VPN, Practice #6 doesn't have a theoretical section defined in the same way as in previous practices but provides concepts explanations within the procedures. The practice makes use of the Cisco VPN client to establish a remote IPSec based VPN connection between a remote client and a PIX firewall. To simplify the implementation it was decided that once the connection is established all traffic will be encrypted and go through the VPN tunnel. Future practices or modifications can cover concepts of split tunneling to allow access to networks that don't participate in the secure connection.

Practice #6 was evaluated by two graduate students enrolled in the Advanced Data Communications course. The average time taken by the students to complete the practice

was 50 minutes and the instructor assistance (4 times) was required in the following areas:

1. Commands explanations.
2. Concepts explanations.

Some corrections related to guide procedures and observations related to the activity review sheet were done during the course of the practice. The practice received a positive review from the students obtaining an average of 5 in a five points scale for all of the items evaluated. Recommendations from the students include the addition of screenshots to the section concerning the configuration of the VPN client, the addition of page numbers and the need of lectures and coursework prior to the development of the laboratory practice. Based on its contents, Practice #6 might be implemented in a network security course after the implementation of a practice #3 in the area of VPN. Since this practice only uses one PIX firewall this limits the amount of students that can perform the practice at the same time to two. It is recommended to do this practice in conjunction with practice #7.

Laboratory Practice #7

The title of this practice is "Introduction to AAA Protocols and RADIUS Servers". This practice allows the students to become familiar with the basic settings of a RADIUS server and provides a general idea of how the users are authenticated under a RADIUS scheme. The practice makes use of the Linux FreeRADIUS server and the NTRadPing test utility. The students access the debug mode of the server and introduce NAS and users information to be processed by the RADIUS server.

Due to time constrains, this practices was only implemented by the instructor. The estimated time to complete Practice #7 is 45 minutes. Since there is currently just one RADIUS server the maximum amount of students that can perform this practice at the same time is limited to 2. In the case of a larger group of students, it would be recommended to perform this practice in combination with practice #6 in order to have small groups for this practice.

Laboratory Practice #8

This practice is titled "Implementing RADIUS authentication in NAS" and is a direct continuation of Practice #7 covering the process of configuring the perimeter firewall and the Cisco 2800 Series routers working as APs. While this practice addresses the integration of NAS in the RADIUS infrastructure it also covers the topic of basic implementation of EAP authentication framework using WEP encryption and the Lightweight Extensible Authentication Protocol (LEAP) implementation methodology.

Because of time limitations and students availability issues, this practice was only implemented by the instructor. In terms of instructions per device, this is the shortest practice and the time to complete it has been estimated to be 40 minutes for groups of students working in different devices. To ensure that the EAP implementation is presented to all students, the students working with the firewall will need to work together with the students working with the Cisco 2800 to observe the configuration of the EAP parameters.

Chapter 5

Conclusions

The purpose of this thesis was the development of laboratory practices for the deployment of a network that could exemplify the current industry needs and in this way establish the basis for an improved computer networking curriculum. Overall, the hypethesis presented in the Chapter 1 have been proven true, and the objectives have been acomplished. The following conclusions are a comparative view between the purpose and objectives of the study and the results obtained from the development of the practices and the evaluations provided by the students.

Additional Theoretical Background

This thesis intended to provide an additional theoretical background for the students through the execution of the laboratory practices. Overall, the students' impression regarding the theoretical explanations presented in the laboratory practices has been positive. While it is important to consider that the sample taken for the evaluation is limited, it is also necessary to indicate that the laboratory practices don't intend to work as a substitute for a proper class lecture in the subject but intend to work as complementary material for a formal course.

Comprehensive and Easy to Understand Laboratory Procedures

From the evaluation of the students presented in Appendix C it can be concluded that the procedures presented in the laboratory practices have been easy to follow and understand. It is important to notice that although the students who participated in the practices' evaluation have some background in computer networking, most of the concepts covered in the laboratory practices were new to them, which highlights the fact

that the procedures are easy to follow by persons who are being introduced in the topics covered in the practices.

Highlighting Similarities with Real Life Scenarios

While a network in a laboratory environment presents significant differences from a real life network, the implementation of services in the network and the overall topology modifications presented in each laboratory practice allow the laboratory network to share many similarities to a real business network that slowly grows and incorporates more services to its existing infrastructure. The inclusion of more equipment and services in the future as well as further modifications to the new topology might allow the telecommunication laboratory network to resemble more closely a real life scenario.

Optimization of the Laboratory Equipment

The development of the new set of laboratory practices has improved the use of the laboratory equipment by incorporating new devices to the existing topology and developing laboratory practice that promote the use of these devices by the students.

Appendix F presents the final version of each laboratory practice after the evaluation of the students and modifications from the instructor. It is important to consider that some of these practices can be incorporated in the existing curriculum and that the current laboratory topology allows the development of future practices in the areas of VoIP, Wireless networks and Network security. The laboratory could be further improved to implement a specialized curriculum or course in the previously mentioned areas depending on the demand, which will require further modifications to the laboratory topology and the incorporation of new equipment.

References

Association for Computing Machinery [ACM] & IEEE Computer Society, Interim CS2008 Review Taskforce (2008). *Computer science curriculum 2008: An interim revision of CS 2001*. Retrieved March 7, 2011, from http://www.acm.org//education/curricula/ComputerScience2008.pdf

Bhaiji, Y. (2008). *Network security technologies and solutions.* Indianapolis, IN: Cisco Press.

Burgess, M. (2000). *Principles of network and system administration.* Chichester, England: John Wiley & Sons, Ltd

Biggs, J. (2004). *Black hats: Misfits, criminals, and scammers in the Internet age.* New York, NY: Apress.

Cioara, J., Cavanaugh, M. J., & Krake, K. A. (2009). *CCNA voice official exam certification guide*. Indianapolis, IN: Cisco Press.

Cisco Systems, et al. 2004. *Internetworking technologies handbook* (4th ed.) [Electronic resource]. Retrieved from http://proquestcombo.safaribooksonline.com/1587051192

Davidson, J.,Peters, J., Bhatia, M., Kalidindi, S., & Mukherjee, S. (2006). *Voice over IP fundamentals* (2nd ed.) [Electronic resource]. Retrieved from http://proquestcombo.safaribooksonline.com/1587052571

Deal, R. A. (2002). *Cisco Pix firewalls*. Emeryville, CA: McGraw-Hill/Osborne.

Dekleva, S., Shim, J. P., Varshney, U., & Knoerzer, G. (2007). Evolution and Emerging Issues in Mobile Wireless Networks. *Communications of the ACM*, 50(6), 38-43.

Fung, K. T. (2005). *Network security technologies* (2nd ed.). Boca Raton, FL: CRC Press LLC.

Gautschi, T. (1995). Embracing information age change. *Design News*, *51*(6), 186. Retrieved October 15, 2009, from Academic Search Premier database http://search.ebscohost.com

Geier, J. (2010. *Designing and deploying 802.11n wireless networks*. Indianapolis, IN: Cisco Press.

Gibbs, M., Bastien, G., Carter, E. & Degu, C., A. (2006). *CCSP SNPA official exam certification guide* (3rd ed.). Indianapolis, IN: Cisco Press.

Gregg, M. (2008). *Build your own security lab: a field guide for network testing*. Indianapolis, IN: WileyPublishing, Inc.

Hens, F. J., & Caballero, J. M. (2008). *Triple play: Building the converged network for IP, VoIP and IPTV.* Chichester, England: John Wiley & Sons Ltd.

Kasera, S., Narang , N., & Narang, S. (2007). *Communication networks : principles and practice*. New York, NY: McGraw-Hill

Macaulay, T. (2006). *Securing converged IP networks*. Boca Raton, FL: Auerbach Publications.

Parker, D. (2008). Skills for the Future. *SecurityFocus*. Retrieved March 2, 2001, from http://www.securityfocus.com/columnists/464/1

Paulson, L. (2002). Wanted: More Network-Security Graduates and Research. *Computer,* 35(2), 22. Retrieved March 17, 2011, from http://www.just.edu.jo/~tawalbeh/nyit/incs741/wanted-security.pdf

Sarkar, N. (2006). Teaching Computer Networking Fundamentals Using Practical Laboratory Exercises. *IEEE Transactions on Education*, *49*(2), 285-291

Sarkar, N. I., & Craig, T. M. (2006). Teaching Wireless Communication and Networking Fundamentals Using Wi-Fi Projects. *IEEE Transactions on Education*, *49*(1), 98-104.

Tang, Y., Draper, T., Xu, Z. (2008). H*yperlab: towards building a hybridized and adaptive remote computer networking laboratory.* Retrieved March 18, 2011, from the School of Information Technology at Illinois State University website: http://www.itk.ilstu.edu/faculty/ytang/TR-Hyperlab-ytang.pdf

Thomas, T. H. II, Freeland, E. J., Coker, M., & Stoddard, D. A. (2001). *Designing Cisco networks*. McGraw-Hill.

Turban, E., Leiden, D., McLean, E., & Wetherbe, J. (2008). *Information technology for management* (6th ed.). Hoboken, New Jersey: John Wiley & Sons, Inc.

Wilton, A., & Charity, T. (2008). *Deploying Wireless Networks*. Cambridge, England: Cambridge University Press.

Appendices

This section contains all additional material related to the study. It has been divided in six parts as follows:

1. Appendix A: Definition of Terms
2. Appendix B: Evaluation Sheets
3. Appendix C: Evaluation Results
4. Appendix D: Server Configuration Guidelines
5. Appendix E: Guidelines for the Instructor
6. Appendix F: Laboratory Practices

Appendix A

Definition of Terms

This study covers many concepts in the areas of network and network security. The following is a list of terms presented in this document:

Authentication –*Process of confirming that an individual is who it claims to be.*

Authentication, authorization and accounting (AAA) Protocols –*A set of network protocols that ensure access control in the form of authentication, authorization and non-repudiation on network devices and network services.*

Authorization –*Process of specifying the resources and services that an individual can access in a network.*

Denial of services (DoS) Attack –*A type of IT security attack with the objective of making a network resource or service unavailable to its intended users.*

DIAMETER –*A network protocol that provides AAA services, intended to substitute RADIUS, not fully implemented.*

Encryption –*The process of making information unreadable by means of a cipher algorithm. The information can be retrieved by means of a key.*

Extensible Authentication Protocol (EAP) –*A protocol for authentication which defines message formatting and different authentication mechanisms. This protocol needs to be encapsulated by means of a different protocol.*

Global System for Mobile Communication –*The most common standard for mobile telephony networks.*

IEEE 802.1Q –*A standard that defines the use of VLANs. It is used for the sharing of a single network link by many logical networks.*

IEEE 802.11 –*A set of standards that establish the guidelines for Wireless LANs (WLANs). Also known as Wi-Fi.*

IEEE 802.11x –*A networking standard designed to provide network access control in the form of authentication mechanisms for LANs and WLANs.*

Internet Key Exchange (IKE) –*An IPsec protocol used to establish security attributes in a two way communication.*

Internet Protocol Security (IPsec) –*A suit of protocols used to provide security for IP based communication.*

Lightweight Extensible Authentication Protocol (LEAP) –*A CISCO proprietary methodology for EAP implementation. It uses dynamic WEP for encryption although it can be implemented in WPA.*

Local Area Network(LAN) –*A computer network that connects different devices in a relatively small area, such as a single building or between various close buildings.*

Metropolitan Area Network (MAN) –*A large computer network that can cover a city or a large campus area, interconnecting LANs and WANs.*

Network access server (NAS) –*A device that manages the access to a network and the network resources.*

Non-repudiation –*The act of keeping track of the activities that users perform in the network to avoid the dispute or repudiation of their actions.*

Public Switched Telephone Network (PSTN) –*The collection of all the networks that handle the public telephone services*

Quality of Service (QoS) –*The ability of network devices to provide different priority to certain types of data and applications in accordance to the rules established by the network administrator.*

Radio Channel –*A set of frequencies established for radio communications.*

Remote authentication dial-in user service (RADIUS) –*A standard protocol that provides AAA services.*

Service Set Identifyer –*A tag used by the access point to identify a WLAN.*

Terminal access controller access-control system plus (TACACS+) –*A proprietary protocol developed by Cisco Systems to provide AAA services.*

Triple Play –*A telecommunication/marketing term used for the provisioning of telephone, TV and data services over a single connection*

Virtual private network (VPN) –*A computer network implemented outside the basic corporate network with the purpose of extending it scope to external users or other locations.*

Wide Area network (WAN) –*A computer network that can cover many cities and even countries, it is formed by the combination of many smaller networks known as local area networks.*

Wireless Network –*Any type of communication or computer network that works without the use of wires, either by radio signals or other types or waves.*

Wireless Local Area Network –*A wireless network that links different devices in a small area, usually by means of IEEE 802.11 protocols.*

Wired Equivalent Privacy (WEP) –*A security algorithm that intends to provide confidentiality for wireless networks. It has been deprecated but it's still widely used.*

Wi-Fi Protected Access (WAP) –*A security protocol intended to replace WEP. It complies with the security specifications defined by IEEE 802.11i.*

WiMAX –*A telecommunication protocol designed for the implementation of Wireless MANs, intended as an alternative for Cable/DSL Internet access.*

ZigBee –*A wireless specification offering low cost with a long battery life for low performance application for short to medium range transmission. An alternative to Bluetooth.*

APPENDIX B

EVALUATION SHEETS

INSTRUCTOR EVALUATION SHEET

Practice Started at: _____

Time to finish the Practice (In case all students are doing the same procedure)

Student #1: _____

Student #2: _____

Student #3: _____

Student#4: _____

Student#5: _____

Of times when instructor assistance was needed. _____

Type of assistance provided:

_____

_____

Observations:

_____

_____

LABORATORY PRACTICE EVALUATION

Please indicate in a scale from 1 (poor) to five (Excellent) your impression in relation to the laboratory practice you finished.

1. Were the objectives properly explained?

1	2	3	4	5

2. Were the network diagrams useful in the understanding of the practice?

1	2	3	4	5

3. Were the theoretical explanations easy to understand?

1	2	3	4	5

4. Were the procedures easy to understand?

1	2	3	4	5

5. After finishing the practice, do you consider the initial objectives were accomplished?

1	2	3	4	5

6. Would you recommend the use of this practice?

1	2	3	4	5

7. What things could be changed or improved in relation to this practice?

_____

_____

_____

_____

Appendix C

Evaluation Results

Table 1

Evaluation results for Practice #1

Instructor Evaluation	
Number of Students	3
Average Completion time	1 hour 15 minutes
Times when assistance was required	6
Observations	Additional explanations were required regarding how to complete the Review Sheet.

Students Evaluation	
Area Evaluated	**Average Score**
Explanation of objectives	4.67
Utility of diagrams	5
Theoretical explanations	4.67
Explanation of procedures	5
Accomplishment of objectives	5
Recommendation for future use	5

Table 2

Evaluation results for Practice #2

Instructor Evaluation	
Number of Students	5
Average Completion time	30 minutes (No review sheet)
Times when assistance was required	5
Observations	It was necessary to specify the troubleshooting commands. After finishing the practice it was concluded that the creation of review sheets for testing and troubleshooting were needed for future practices. The evaluation sheets needed to be modified.

Students Evaluation	
Area Evaluated	**Average Score**
Explanation of objectives	4.4
Utility of diagrams	3.8
Theoretical explanations	4
Explanation of procedures	4.4
Accomplishment of objectives	4.2
Recommendation for future use	4.2

Table 3

Evaluation results for Practice #3

Instructor Evaluation	
Number of Students	3
Average Completion time	45 minutes
Times when assistance was required	6
Observations	Pings to network address 10.0.0.0 were successful from the internal network. Routemap configuration required corrections Last two questions in the activity review sheet required corrections.

Students Evaluation	
Area Evaluated	**Average Score**
Explanation of objectives	5
Utility of diagrams	4.67
Theoretical explanations	5
Explanation of procedures	5
Accomplishment of objectives	5
Recommendation for future use	5

Table 4

Evaluation results for Practice #4

Instructor Evaluation	
Number of Students	2
Average Completion time	1 hour 13 minutes
Times when assistance was required	6
Observations	Corrections in Part II, step 1 and Part III, step 2. Last question in the review sheet might be confusing for students with no background.

Students Evaluation	
Area Evaluated	**Average Score**
Explanation of objectives	4.5
Utility of diagrams	3.5
Theoretical explanations	4
Explanation of procedures	5
Accomplishment of objectives	5
Recommendation for future use	5

Table 5

Evaluation results for Practice #5

Instructor Evaluation	
Number of Students	4
Average Completion time	50 minutes
Times when assistance was required	5
Observations	Frequency used by the radio interface could be identified by the student as part of the review process.

Students Evaluation	
Area Evaluated	**Average Score**
Explanation of objectives	5
Utility of diagrams	5
Theoretical explanations	4.75
Explanation of procedures	4.5
Accomplishment of objectives	5
Recommendation for future use	5

Table 6

Evaluation results for Practice #6

Instructor Evaluation	
Number of Students	2
Average Completion time	50 minutes
Times when assistance was required	4
Observations	Web browser cache of the remote client needs to be erased before the start of the practice The site-to-site reference in Part II step 4 needed to be corrected. Pages need to be numbered.

Students Evaluation	
Area Evaluated	**Average Score**
Explanation of objectives	5
Utility of diagrams	5
Theoretical explanations	5
Explanation of procedures	5
Accomplishment of objectives	5
Recommendation for future use	5

Appendix D

Server Configuration Guidelines

This document presents procedures to configure the different services required by the Telecommunication Laboratory in a computer running OpenSUSE 11.3 Operative System. It is assumed that a basic installation of OpenSUSE has been performed in the computer prior to the implementation of these procedures, that the computer has an internet connection to download software from the internet and that the user posses some knowledge of Linux Operative Systems. Unlike other Linux distributions OpenSUSE offers a very intuitive control center called YaST, which allows the user to easily manage and configure most of the basic server components. The following website include guidelines regarding the installation of OpenSUSE 11.3:

http://en.opensuse.org/SDB:DVD_installation_for_11.3

In most cases, software installation will be performed through YaST Software Manager. Software can also be searched on-line through webpin. To install software with YaST Software Manager the following steps are needed:

1. Click on the application launcher.
2. Go to Computer and Click on YaST.
3. Click on Software and select Software Management. Go to the Search tab and enter the name of the software to be installed.
4. Select the appropriate packages to be installed and their dependencies.

Configuring RADIUS and Dial-Up Admin

The following steps are needed to configure FreeRADIUS and its GUI Dial-up admin on OpenSUSE. The following packets must have been installed beforehand with

YaST Software Manager: FreeRadius Client and Server, FreeRadius Server Dialup Admin, Apache, PHP, Perl and Date-Manip Perl Module. The password *yrms5m0s* was set up for most accounts with administrative priviledges unless specified. All the instructions are case-sensitive.

Step 1: Configure Apache HTTP Server.

Click on the application launcher. Go to Computer and Click on YaST. Click on Network Services and then click on HTTP Server. The service must be enabled and the port must be open in the firewall or the latter must be deactivated.

Click on Server Modules and make sure that both Perl and PHP5 are enabled.

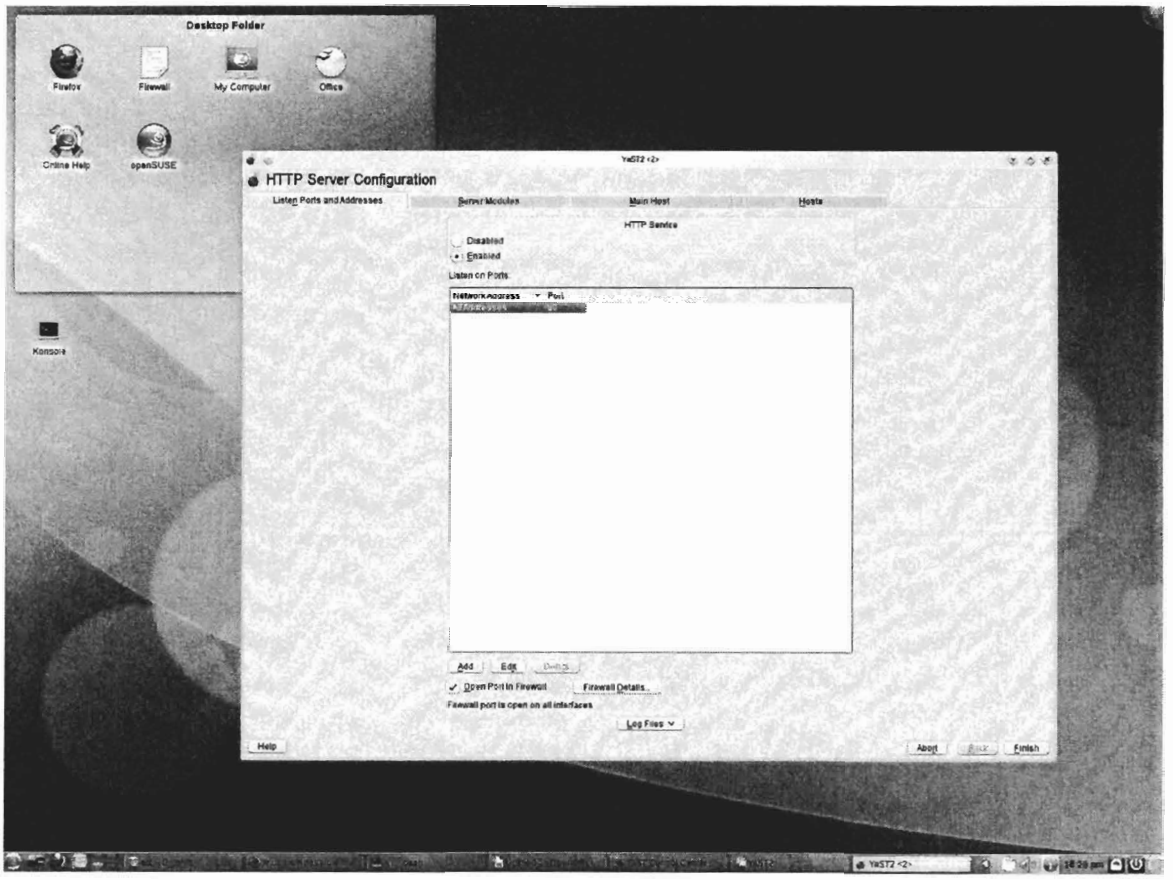


Figure 1. Apache Web Server configuration menu.

Click on Main Host and double click on "Directory" with a value of "/srv/www/htdocs". Select the Option "Options" and add the folowing value: FollowSymLinks. This will allow the establishment of symbolic links between the APACHE server HTDOCS and the dialupadmin HTDOCS . Open a Web browser and type in the address space: http://localhost/ It must prompt you to a webpage indicating that it works.

Step 2: Install and Configure MySQL

MySQL will be used to manage users and NAS information in RADIUS. In YaST click on System and then click on "System Services (RunLevel)". Make sure that both FreeRadius and MySQL are running. Enable the services if needed.

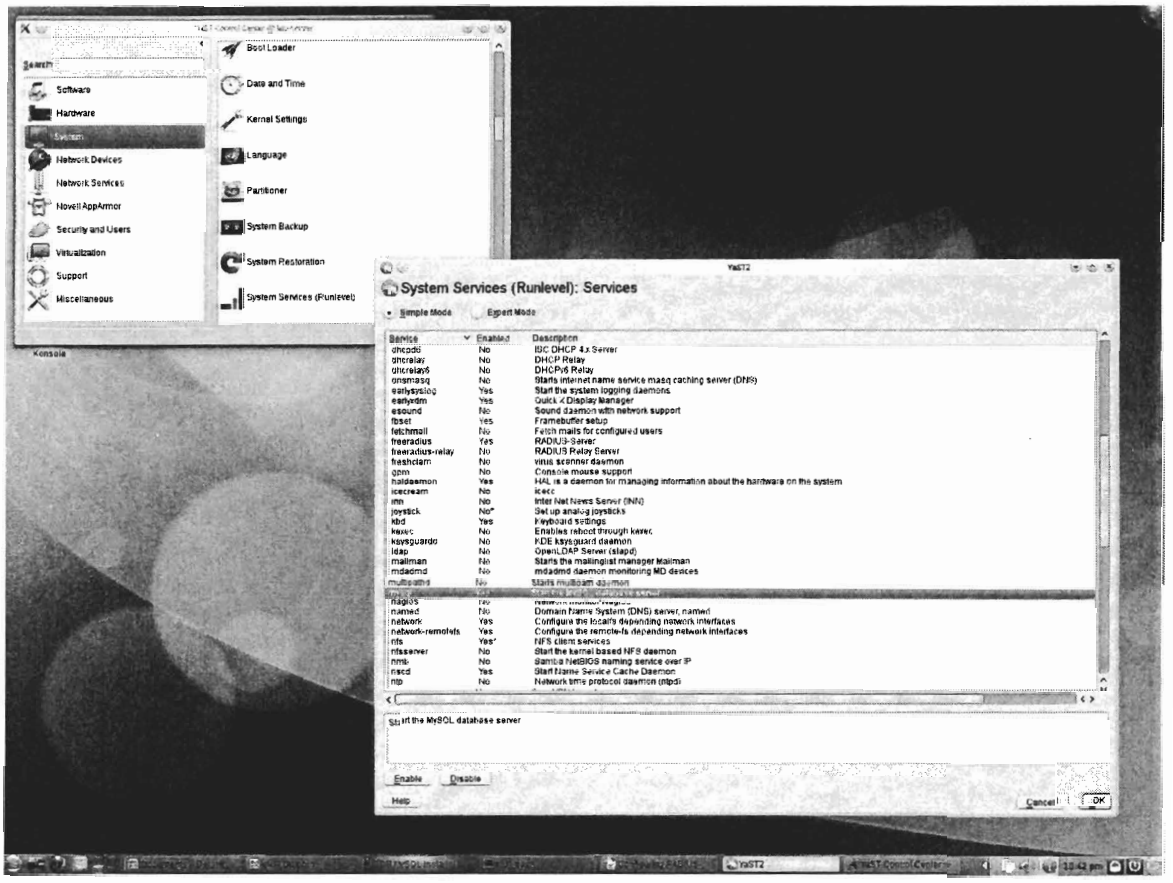


Figure 2. System Services (RunLevel)

Download and install PHPMyAdmin to graphically configure MySQL, from the following website:

http://software.opensuse.org/ymp/server:php:applications/openSUSE_11.3/phpMyAdmin.ymp

A wizard will open. Follow the instructions of the Wizard to install the package. Open a web browser and enter the following url: http://localhost/phpMyAdmin/ If you have previously defined an username and password, enter them now. Otherwise enter as root without password and define your password in the front page.

Step 3: Configuring Dial-up Admin

The first thing to do is to establish a Virtual Link between the Dial-upAdmin HTDOCS directory and the APACHE HTDOCS directory. Open a console session. Type su and hit enter. It will ask you for the root/administrator password enter the password and after getting access to superuser mode type the following command that will link both directories:

ln -s /usr/share/dialup_admin/htdocs/ /srv/www/htdocs/dialup

In case of problems with the permissions, type the following command to grant access permissions:

sudo chmod 755 /srv/www/htdocs/dialup

Use the APACHE password utility to create a password for the website:

sudo htpasswd2 -cb /srv/www/.htpasswd Administrator yrms5m0s

By doing this, the users will need to enter the username Administrator and password *yrms5m0s* to access the website.

Define the route to the dialupadmin files in the Apache configuration. On the console session open a Dolphin interface as superuser by entering the following command:

kdesu dolphin

Go to /etc/apache2/conf.d/ and open the file radius.conf

Comment all the entries in the file by adding a # symbol before each line. Add the following configuration in the file:

```
<Directory /srv/www/htdocs/dialup/>
  Options FollowSymlinks
  AuthName "Restricted Area"
  AuthType Basic
  AuthUserFile /srv/www/.htpasswd
  require valid-user
  order allow,deny
  allow from all
</Directory>
```

Configure the PHP module in Apache to open php3 files. Using the same superuser Dolphin interface that was opened in the previous step, go to: /etc/apache2/conf.d/ and open the php5.conf file. Modify the configuration so that it looks as follow:

```
<IfModule mod_php5.c>
    AddHandler application/x-httpd-php .php3
    AddHandler application/x-httpd-php .php4
```

```
AddHandler application/x-httpd-php .php5
AddHandler application/x-httpd-php .php
AddHandler application/x-httpd-php-source .php3s
AddHandler application/x-httpd-php-source .php4s
AddHandler application/x-httpd-php-source .php5s
AddHandler application/x-httpd-php-source .phps
DirectoryIndex index.php3
DirectoryIndex index.php4
DirectoryIndex index.php5
DirectoryIndex index.php
</IfModule>
```

Step 4: Create a RADIUS Database

Go to MySQL localhost and type *radius* below "Create a new database". Click on create.

Create the databases from the sqlfiles in the Dialupadmin directory: /usr/share/dialup_admin/sql/mysql/ Open a console session and enter the following command:

```
mysql -h 127.0.0.1 -u root -p
```

It will ask you for the password you specified for root and then you will gain access to mysql. You have to access the radius database by entering the following:

```
mysql> use radius;
```

Enter the following commands to create the databases:

```
mysql> source /usr/share/dialup_admin/sql/mysql/badusers.sql;
```

mysql> source /usr/share/dialup_admin/sql/mysql/mtotacct.sql;

mysql> source /usr/share/dialup_admin/sql/mysql/totacct.sql;

mysql> source /usr/share/dialup_admin/sql/mysql/userinfo.sql;

If there are problems with the last line. Open the file as super user (with the kdesu dolphin method) erase the DEFAULT '0' in the ID line and do it again.

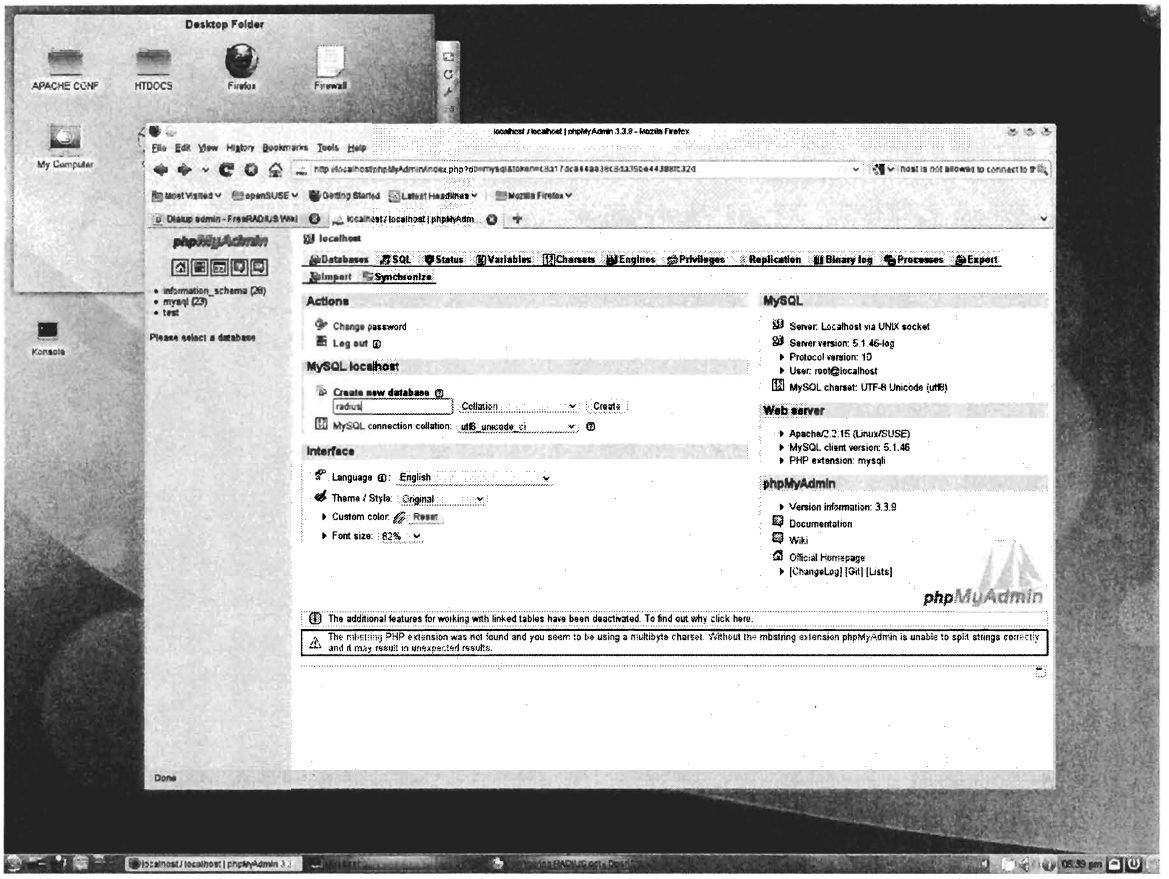


Figure 3. Creating the RADIUS database in phpMyAdmin

After completing the process, create the databases for FreeRADIUS by doing the following:

mysql> source /etc/raddb/sql/mysql/schema.sql;

mysql> source /etc/raddb/sql/mysql/nas.sql;

mysql> commit;

Create a user with privileges on the radius database. Enter the following commands from the mysql prompt:

mysql> create user 'radadmin'@'localhost' identified by 'radlab4411';

mysql> grant all privileges on radius.* to 'radadmin'@'localhost' identified by 'radlab4411' with grant option;

mysql> create user 'radadmin'@'%' identified by 'radlab4411';

mysql> grant all privileges on radius.* to 'radadmin'@'%' identified by ' radlab4411' with grant option;

mysql> flush privileges;

Step 5: Verify the Dial-Up Admin configuration file

The path to the file is /usr/share/dialup_admin/conf/ and the file is admin.conf. You need super user privileges to modify it. The following are the fields that have to be checked, if the value is different or is commented, change it to the value that appears here. This was in accordance to the default OpenSUSE configuration:

general_base_dir: /usr/share/dialup_admin

This is the directory where dialup_admin is installed

general_radiusd_base_dir: /usr/sbin/

This is the directory where FreeRadius is installed

general_domain: cerveau.com

After verifying the previous line, make sure that the following lines in the file are not commented:

general_strip_realms: yes

general_realm_delimiter: @

general_realm_format: suffix

general_lib_type: sql

general_finger_type: snmp

general_radclient_bin: /usr/bin/radclient

The last line must be changed to the specified content. The original content was: general_radclient_bin: %{general_radiusd_base_dir}/bin/radclient

The following information will be used from the server check page so the parameters need to be defined acordingly:

general_test_account_login: UserTest

general_test_account_password: test123

general_radius_server: localhost

general_radius_server_port: 1812

general_radius_server_auth_proto: chap

general_encryption_method: clear

general_radius_server_secret: testing123

general_auth_request_file: %{general_base_dir}/conf/auth.request

general_raddb_dir: /etc/raddb

The following are parameters regarding the conection to the sql server, they must be exactly as they are below:

sql_type: mysql

sql_server: localhost

sql_port: 3306

sql_username: radadmin

sql_password: radlab4411

sql_database: radius

sql_accounting_table: radacct

sql_badusers_table: badusers

sql_check_table: radcheck

sql_reply_table: radreply

sql_user_info_table: userinfo

sql_groupcheck_table: radgroupcheck

sql_groupreply_table: radgroupreply

sql_usergroup_table: radusergroup

sql_total_accounting_table: totacct

sql_nas_table: nas

sql_password_attribute: ClearText-Password

Step 6: Configuring FreeRadius

All these procedures must be performed as super user unless specified otherwise. Open the file: /etc/raddb/clients.conf to create a NAS account for testing:

client localhost {

ipaddr = 127.0.0.1

secret = testing123

shortname = localhost

nastype = other }

Open the file /etc/raddb/users and add the following line to create a user for testing:

UserTest Cleartext-Password := "test123"

Open the file: /etc/raddb/radiusd.conf The following line must not be commented:

$INCLUDE sql.conf

Open the file: /etc/raddb/sql.conf as superuser. Check the following parameters exist in the configuration and if they do, verify that they are not commented:

database = "mysql"

server = "localhost"

login = "radadmin"

password = "radlab4411"

Open the file: /etc/raddb/sites-available/default and check that the option "sql" is not commented in both authentication and accounting.

To test that the server is working properly. Enter the following commands from the command line:

sudo /etc/init.d/freeradius stop

sudo /usr/sbin/radiusd -X

This will start the Radius server in Debug mode. Open a different command line window and type the following:

radtest UserTest test123 localhost 10 testing123

To test that the SQL authentication is working properly, create a user account with Dial-Up Admin. Go to Edit User and type the username (Not the real name but the nickname). Go to Test and type the password that you specified when creating the user.

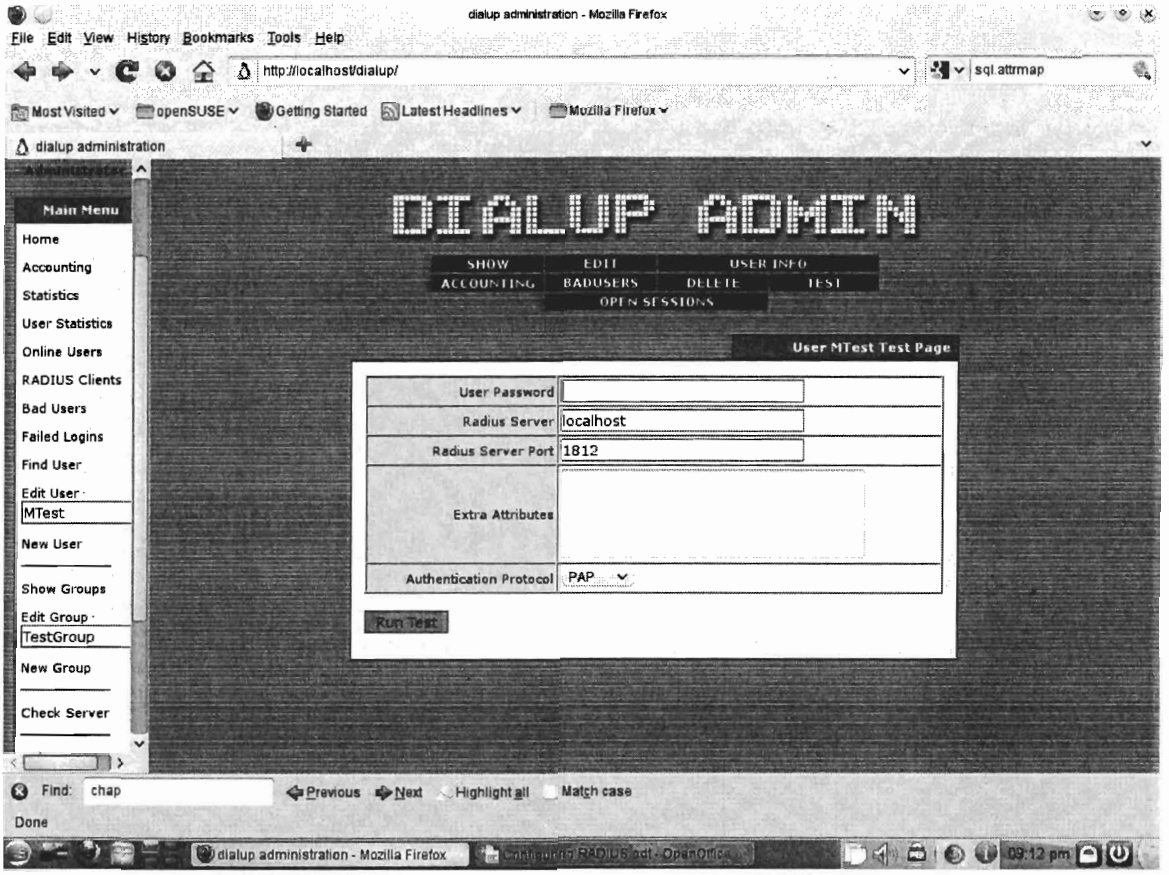


Figure 4. Testing a Database user with Dial-Up Admin

Configuring a DHCP Server

The first step in configuring the DHCP server is to activate the service through YaST. After the service has been activated, the fastest way to configure DHCP is to modify the dhcpd.conf file located in /etc/. The following parameters need to be added in the file:

option domain-name "cerveau.com";

option domain-name-servers 172.16.0.2, 172.16.0.3;

max-lease-time 259200;

```
ddns-updates off;

subnet 172.16.0.0 netmask 255.255.255.0 {
 range 172.16.0.4 172.16.0.125;
 default-lease-time 172800;
 max-lease-time 259200;
}
subnet 192.168.1.0 netmask 255.255.255.0 {
 option routers 192.168.1.1;
 range dynamic-bootp 192.168.1.2 192.168.1.254;
}
subnet 192.168.2.0 netmask 255.255.255.0 {
 option routers 192.168.2.1;
 range dynamic-bootp 192.168.2.2 192.168.2.254;
}
subnet 192.168.3.0 netmask 255.255.255.0 {
 option routers 192.168.3.1;
 range dynamic-bootp 192.168.3.2 192.168.3.254;
}
subnet 192.168.4.0 netmask 255.255.255.0 {
 option routers 192.168.4.1;
 range dynamic-bootp 192.168.4.2 192.168.4.254;
}
```

```
subnet 192.168.5.0 netmask 255.255.255.0 {
 option routers 192.168.5.1;
 range dynamic-bootp 192.168.5.2 192.168.5.254;
}
subnet 192.168.6.0 netmask 255.255.255.0 {
 option routers 192.168.6.1;
 range dynamic-bootp 192.168.6.2 192.168.6.254;
}
```

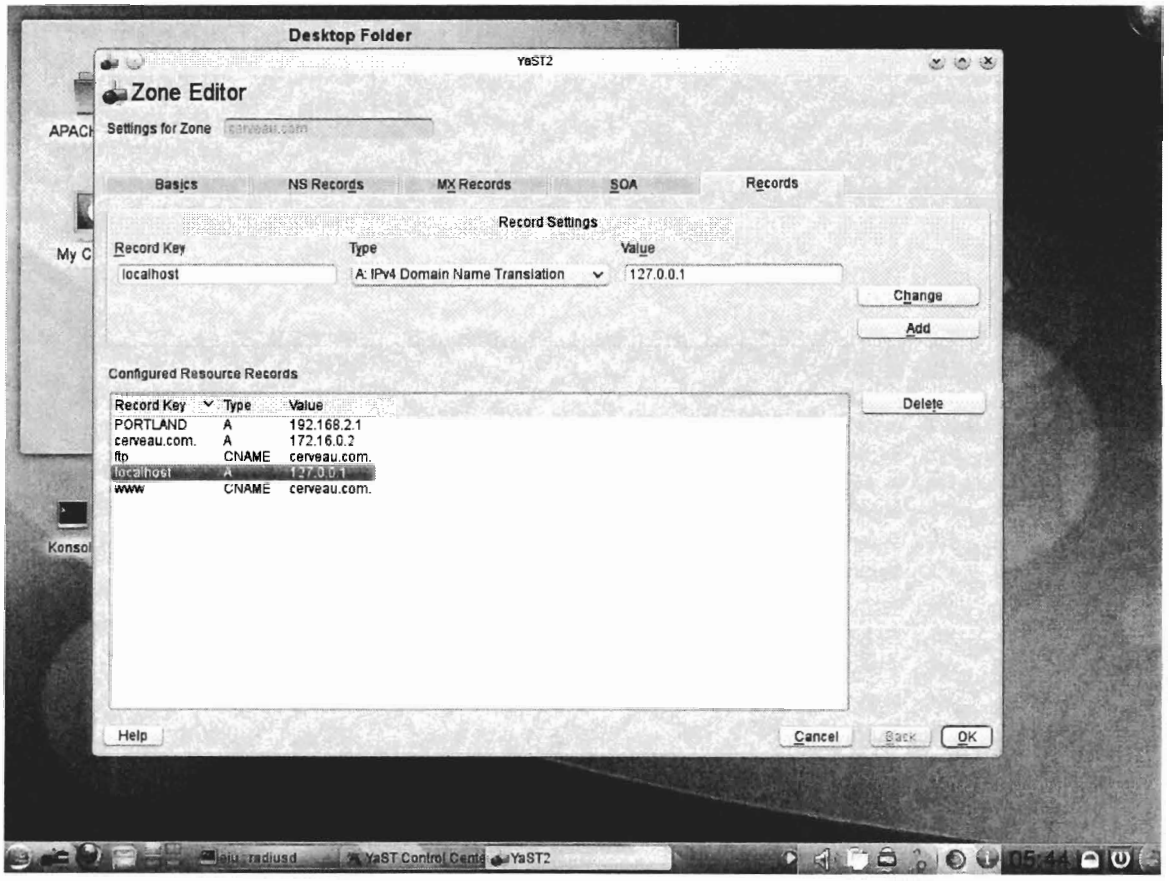


Figure 5. Configuring DNS Records

Configuring a DNS Server

To configure a DNS Server in OpenSUSE follow these steps:

1. Go to Network Services in the YaST Control Center
2. Select DNS Server. Make sure that the Service is configured to start automatically and that is running.
3. Since this is for a laboratory environment and there are no other DNS Servers configured, set the same server as forwarder.
4. Delete any zone in the DNS Zone section. Add the zone cerveau.com as Master DNS zone.
5. Enter the zone editor and go to the NS Records tab. Add localhost.cerveau.com to the name server list.
6. Go to the Record tab and start adding values as presented in Figure 5. Type A indicates a name that will be followed by the DNS suffix cerveau.com. Type CNAME is used to designate prefixes.

Configuring a FTP Server

To configure the FTP Server it is necessary to create a user named ftpuser. The user will belong the the ftp group and will have /home/ftp/ftpuser/ as its home directory. After this user has been created. Follow these steps:

1. Go to Network Services in the YaST Control Center and select FTP Server to configure it.
2. Go to General Settings and mark Chroot Everyone.
3. Define /home/ftp/anon/ as the directory for anonymous users.

4. Enable both anonymous and authenticated users in the system and mark to option upload to allow authenticated users to upload files.
5. Enable passive mode and set the port range that will be used: Between 1024 and 1030.

Configuring Static Routing

To set up static routing in OpenSUSE follow these steps:

1. Go to network settings in the YaST Control Center.
2. Go to the Routing Tab, add the desired routes to the routing table, and mark Enable IP forwarding. For this case, the routes can be seen in Figure 5

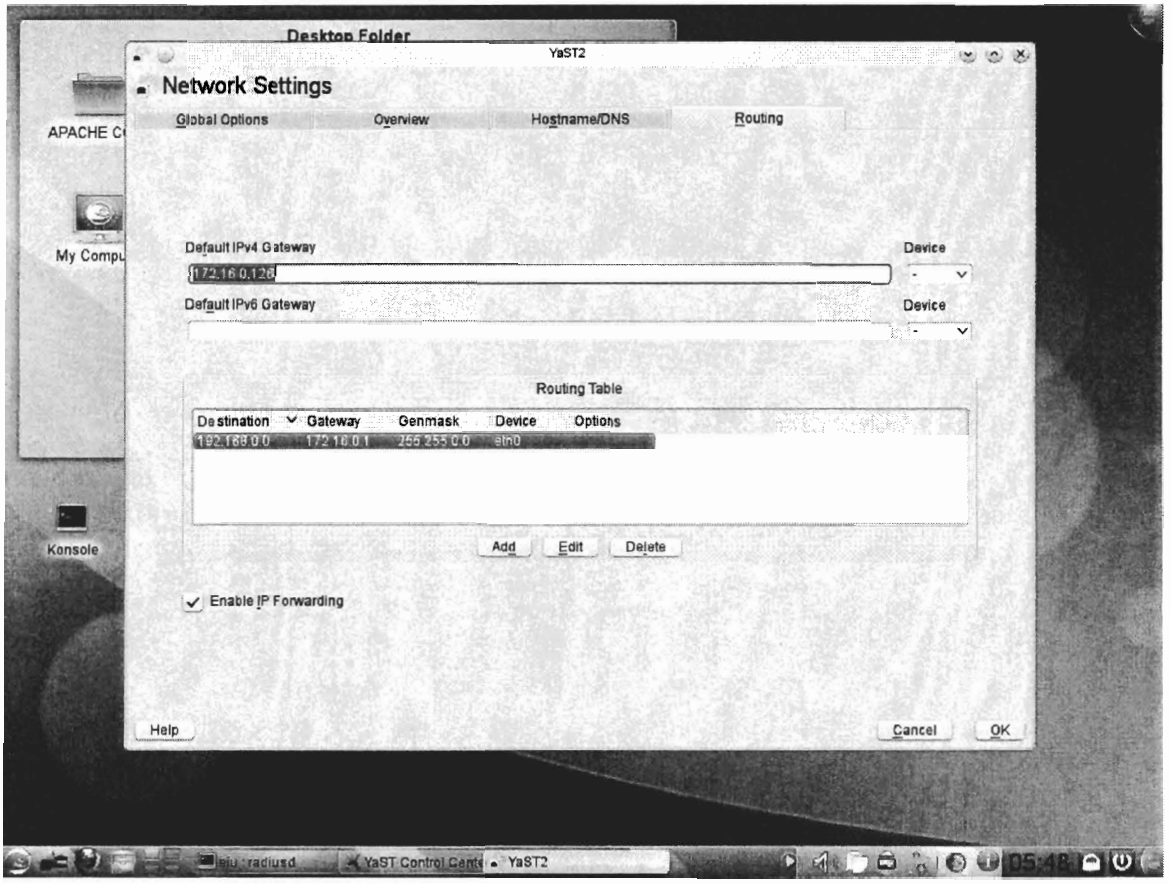


Figure 6. Configuration of static routes

Appendix E

Guidelines for the Instructor

The following are guidelines regarding the activities that the instructor taking care of any laboratory practice needs to perform prior to the implementation of any practice by the students.

This document is divided in sections; the first section contains the configuration files of the internal network which was the starting laboratory topology. Each subsequent section covers aspects related to the preliminary configuration of the new network, commands used, and any additional detail of a particular practice. The practice implementation is progressive, which means that, unless specified, each practice requires the correct implementation of the previous practices. The instructor might enter the configuration commands of any previous practice if the practice to be implemented is being executed as a standalone practice. In order to enter the configuration copy the commands in a notepad file and then paste them in the console during configuration mode.

Internal Network Configuration

Changes to the original network include the IP addresses range, the inclusion of a FTP username and password to access the FTP server, and the inclusion of a DHCP helper address that points to the server in the DMZ.

LOS ANGELES Router

```
service password-encryption
hostname LOS_ANGELES
enable secret class
```

```
ip ftp username ftpuser
ip ftp password ftlab4411
interface Ethernet0
 ip address 192.168.1.1 255.255.255.0
ip helper-address 172.16.0.2
 no shutdown
interface Ethernet1
 ip address 192.168.240.25 255.255.255.252
 no shutdown
interface Serial0
 ip address 192.168.240.1 255.255.255.252
clockrate 500000
no shutdown
interface Serial1
 ip address 192.168.240.22 255.255.255.252
no shutdown
router eigrp 1000
 redistribute static
 network 192.168.1.0
 network 192.168.240.0
ip route 0.0.0.0 0.0.0.0 192.168.240.26
ip route 172.16.0.0 255.255.0.0 192.168.240.26
line con 0
```

```
 password cisco
 login
line vty 0 4
 password cisco
 login
```

PORTLAND Router

```
service password-encryption
hostname PORTLAND
enable secret class
ip ftp username ftpuser
ip ftp password ftplab4411
interface Ethernet0
 ip address 192.168.2.1 255.255.255.0
 ip helper-address 172.16.0.2
interface Ethernet1
 no ip address
 ip helper-address 172.16.0.2
interface Serial0
 ip address 192.168.240.5 255.255.255.252
clockrate 500000
no shutdown
interface Serial1
 ip address 192.168.240.2 255.255.255.252
```

no shutdown

router eigrp 1000

network 192.168.2.0

network 192.168.240.0

line con 0

password cisco

login

line vty 0 4

password cisco

login

CHICAGO Router

service password-encryption

hostname CHICAGO

enable secret class

ip ftp username ftpuser

ip ftp password ftplab4411

interface Ethernet0

ip address 192.168.3.1 255.255.255.0

ip helper-address 172.16.0.2

no shutdown

interface Serial0

ip address 192.168.240.9 255.255.255.252

clockrate 500000

```
no shutdown
interface Serial1
 ip address 192.168.240.6 255.255.255.252
no shutdown
router eigrp 1000
 network 192.168.3.0
 network 192.168.240.0
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
```

NEW YORK Router

```
service password-encryption
hostname NEW_YORK
enable secret class
ip ftp username ftpuser
ip ftp password ftplab4411
interface Ethernet0
 ip address 192.168.4.1 255.255.255.0
ip helper-address 172.16.0.2
no shutdown
```

```
interface Serial0
 ip address 192.168.240.13 255.255.255.252
clockrate 500000
no shutdown
interface Serial1
 ip address 192.168.240.10 255.255.255.252
no shutdown
router eigrp 1000
 network 192.168.4.0
 network 192.168.240.0
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
```

MIAMI Router

```
service password-encryption
hostname MIAMI
enable secret class
ip ftp username ftpuser
ip ftp password ftplab4411
interface Ethernet0
```

```
 ip address 192.168.5.1 255.255.255.0
ip helper-address 172.16.0.2
no shutdown
interface Serial0
 ip address 192.168.240.17 255.255.255.252
 no ip directed-broadcast
 clockrate 500000
no shutdown
interface Serial1
 ip address 192.168.240.14 255.255.255.252
no shutdown
router eigrp 1000
 network 192.168.5.0
 network 192.168.240.0
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
```

ST LOUIS Router

```
service password-encryption
hostname ST_LOUIS
```

```
enable secret class
ip ftp username ftpuser
ip ftp password ftplab4411
interface Ethernet0
 ip address 192.168.6.1 255.255.255.0
ip helper-address 172.16.0.2
no shutdown
interface Serial0
 ip address 192.168.240.21 255.255.255.252
clockrate 500000
no shutdown
interface Serial1
 ip address 192.168.240.18 255.255.255.252
no shutdown
router eigrp 1000
 network 192.168.6.0
 network 192.168.240.0
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
```

Laboratory Practice #1

This practice originally requires a working configuration for both firewalls in the DMZ network since the student will need it at the beginning. The instructor might use the the Practice commands presented below.The following are the preliminary activities that need to be performed:

1. Define a computer as an external network host with the address 16.16.8.8
2. Verify connectivity within the devices participating in the practice, including hosts.
3. Verify the configuration of the routers in the internal network.
4. Verify that FTP, DHCP and DNS services are available.

Firewall HOLLYWOOD01 (PIX 506E) Practice Commands

hostname HOLLYWOOD01

enable password class

interface ethernet0 auto

interface ethernet1 auto

ip address inside 192.168.240.26 255.255.255.252

ip address outside 172.16.0.1 255.255.255.0

route inside 192.168.0.0 255.255.0.0 192.168.240.25 1

route outside 0.0.0.0 0.0.0.0 172.16.0.126 1

access-list NO_NAT_NEEDED permit ip any any

nat (inside) 0 access-list NO_NAT_NEEDED

access-list INCOMING permit icmp any any

access-list OUTGOING permit icmp any any

access-list OUTGOING permit tcp any any eq www

access-list OUTGOING permit tcp any host 172.16.0.2 eq ftp

access-list OUTGOING permit tcp any host 172.16.0.2 range 1024 1030

access-list INCOMING permit udp host 172.16.0.2 eq bootps any

access-list OUTGOING permit udp any eq bootpc host 172.16.0.2

access-list OUTGOING permit udp any eq domain any

access-list OUTGOING permit udp any any eq domain

access-list OUTGOING permit tcp any eq domain any

access-list OUTGOING permit tcp any any eq domain

access-list INCOMING deny ip any any

access-list OUTGOING deny ip any any

access-group INCOMING in interface outside

access-group OUTGOING in interface inside

Firewall HOLLYWOOD02 (PIX 501) Practice Commands

hostname HOLLYWOOD02

enable password class

interface ethernet0 100full

interface ethernet1 100full

ip address inside 172.16.0.126 255.255.255.0

ip address outside 16.16.8.1 255.255.255.0

route inside 192.168.0.0 255.255.0.0 172.16.0.1 1

route outside 0.0.0.0 0.0.0.0 16.16.8.2 1

access-list INCOMING permit icmp any any

access-list OUTGOING permit icmp any any

access-list OUTGOING permit tcp any any eq www

access-list INCOMING permit tcp any any eq www

access-list INCOMING deny ip any any

access-list OUTGOING deny ip any any

access-group INCOMING in interface outside

access-group OUTGOING in interface inside

global (outside) 1 interface

nat (inside) 1 0.0.0.0 0.0.0.0 0 0

static (inside, outside) 16.16.8.4 172.16.0.2

Laboratory Practice #2

Prior to the implementation of this practice, firewall HOLLYWOOD01 and HOLLYWOOD02 are required to have the configuration of Laboratory Practice #1. The configuration of HOLLYWOOD02 will be modified by the instructor to erase the NAT settings defined in Laboratory Practice #1 as indicated in this section. The Cisco 2800 Series routers must be loaded with a basic configuration that includes interfaces' addresses and basic parameters, including static routing; any previous configuration must be erased. Other preliminary activities that must be performed are:

1. Introduce the following static addresses in the Anchorage and Honolulu networks' host:

   Anchorage Host IP Address and Mask: 10.1.0.2 10.1.0.1 255.255.192.0

   Anchorage Host Default Gateway: 10.1.0.1

   DNS Server: 172.16.0.2

   Honolulu Host IP Address and Mask: 10.2.0.2 10.1.0.1 255.255.192.0

Honolulu Host Default Gateway: 10.2.0.1

DNS Server: 172.16.0.2

2. Define a computer as an external network host with the address 16.16.8.8. The default gateway must be the firewall HOLLYWOOD02 outside address.
3. Verify connectivity within the internal network. Hosts within the networks involved in the practice should not reach the external host.

Firewall HOLLYWOOD02 Preliminary Configuration Commands

```
no global (outside) 1 interface
no nat (inside) 1 0.0.0.0 0.0.0.0 0 0
no static (inside, outside) 16.16.8.4 172.16.0.2
```

Router ANCHORAGE Preliminary Configuration Commands

```
hostname ANCHORAGE
enable secret class
service password-encryption
interface fastethernet 0/0
ip address 16.16.8.2 255.255.255.0
no shutdown
interface vlan2
ip address 10.1.0.1 255.255.192.0
no shutdown
interface range fastEthernet 0/1/0 - 3
switchport mode access
switchport access vlan 2
```

line console 0

password cisco

login

line vty 0 807

password cisco

login

ip route 10.2.0.0 255.255.0.0 16.16.8.3

ip route 0.0.0.0 0.0.0.0 16.16.8.1

Router HONOLULU Preliminary Configuration Commands

hostname HONOLULU

enable secret class

service password-encryption

interface fastethernet 0/0

ip address 16.16.8.3 255.255.255.0

no shutdown

interface vlan2

ip address 10.2.0.1 255.255.192.0

no shutdown

interface range fastEthernet 0/1/0 - 3

switchport mode access

switchport access vlan 2

line console 0

password cisco

login

line vty 0 807

password cisco

login

ip route 10.1.0.0 255.255.0.0 16.16.8.2

ip route 0.0.0.0 0.0.0.0 16.16.8.1

Firewall HOLLYWOOD02 Practice Commands

global (outside) 1 interface

nat (inside) 1 0.0.0.0 0.0.0.0 0 0

static (inside, outside) 16.16.8.4 172.16.0.2

Router ANCHORAGE Practice Commands

ip nat pool a_nat 16.16.8.2 16.16.8.2 netmask 255.255.255.0

access-list 1 permit 10.1.0.0 0.0.255.255

ip nat inside source list 1 pool a_nat overload

interface fastethernet0/0

ip nat outside

interface vlan2

ip nat inside

Router HONOLULU Practice Commands

ip nat pool h_nat 16.16.8.3 16.16.8.3 netmask 255.255.255.0

access-list 1 permit 10.2.0.0 0.0.255.255

ip nat inside source list 1 pool h_nat overload

interface fastethernet0/0

ip nat outside

interface vlan2

ip nat inside

Laboratory Practice #3

This practice doesn't require the instructor to configure any network device prior to the students' implementation as long as Laboratory Practice #1 and Laboratory Practice #2 were performed successfully. The instructor will need to verify the following:

1. Proper configuration of NAT/PAT.
2. Hosts in Anchorage and Honolulu networks must have the static addressing scheme presented in Laboratory Practice #2.
3. FTP and DNS should not be available to hosts in Anchorage or Honolulu networks.

Router ANCHORAGE Practice Commands

crypto isakmp enable

crypto isakmp policy 1

authentication pre-share

encryption 3des

hash sha

group 2

lifetime 60000

crypto isakmp key vpnkey4411 address 16.16.8.1

crypto isakmp key vpnkey4411 address 16.16.8.3

crypto ipsec transform-set vpnAnchor esp-3des esp-sha-hmac

exit

```
access-list 101 permit ip 10.1.0.0 0.0.255.255 10.2.0.0 0.0.255.255
access-list 102 permit ip 10.1.0.0 0.0.255.255 172.16.0.0 0.0.255.255
access-list 103 permit ip 10.1.0.0 0.0.255.255 192.168.0.0 0.0.255.255
crypto map vpn_tunnel 1 ipsec-isakmp
match address 101
set peer 16.16.8.3
set transform-set vpnAnchor
exit
crypto map vpn_tunnel 2 ipsec-isakmp
match address 102
set peer 16.16.8.1
set transform-set vpnAnchor
exit
crypto map vpn_tunnel 3 ipsec-isakmp
match address 103
set peer 16.16.8.1
set transform-set vpnAnchor
exit
interface fastethernet 0/0
crypto map vpn_tunnel
access-list 199 deny ip 10.1.0.0 0.0.255.255 10.2.0.0 0.0.255.255
access-list 199 deny ip 10.1.0.0 0.0.255.255 172.16.0.0 0.0.255.255
access-list 199 deny ip 10.1.0.0 0.0.255.255 192.168.0.0 0.0.255.255
```

access-list 199 permit ip 10.1.0.0 0.0.255.255 any

route-map vpn_nat permit 10

match ip address 199

exit

ip nat inside source route-map vpn_nat pool a_nat overload

no ip nat inside source list 1 pool a_nat overload

Router HONOLULU Practice Commands

crypto isakmp enable

crypto isakmp policy 2

authentication pre-share

encryption 3des

hash sha

group 2

lifetime 60000

crypto isakmp key vpnkey4411 address 16.16.8.1

crypto isakmp key vpnkey4411 address 16.16.8.2

crypto ipsec transform-set vpnHono esp-3des esp-sha-hmac

exit

access-list 101 permit ip 10.2.0.0 0.0.255.255 10.1.0.0 0.0.255.255

access-list 102 permit ip 10.2.0.0 0.0.255.255 172.16.0.0 0.0.255.255

access-list 103 permit ip 10.2.0.0 0.0.255.255 192.168.0.0 0.0.255.255

crypto map vpn_tunnel 1 ipsec-isakmp

match address 101

```
set peer 16.16.8.2
set transform-set vpnHono
exit
crypto map vpn_tunnel 2 ipsec-isakmp
match address 102
set peer 16.16.8.1
set transform-set vpnHono
exit
crypto map vpn_tunnel 3 ipsec-isakmp
match address 103
set peer 16.16.8.1
set transform-set vpnHono
exit
interface fastethernet 0/0
crypto map vpn_tunnel
access-list 199 deny ip 10.2.0.0 0.0.255.255 10.1.0.0 0.0.255.255
access-list 199 deny ip 10.2.0.0 0.0.255.255 172.16.0.0 0.0.255.255
access-list 199 deny ip 10.2.0.0 0.0.255.255 192.168.0.0 0.0.255.255
access-list 199 permit ip 10.2.0.0 0.0.255.255 any
route-map vpn_nat permit 10
match ip address 199
exit
ip nat inside source route-map vpn_nat pool h_nat overload
```

no ip nat inside source list 1 pool h_nat overload

Firewall HOLLYWOOD02 Practice Commands

isakmp enable outside

isakmp policy 3 authentication pre-share

isakmp policy 3 encrypt 3des

isakmp policy 3 hash sha

isakmp policy 3 group 2

isakmp policy 3 lifetime 60000

isakmp key vpnkey4411 address 16.16.8.2

isakmp key vpnkey4411 address 16.16.8.3

crypto ipsec transform-set vpnHolly esp-3des esp-sha-hmac

access-list to_anchor1 permit ip 192.168.0.0 255.255.0.0 10.1.0.0 255.255.0.0

access-list to_anchor2 permit ip 172.16.0.0 255.255.0.0 10.1.0.0 255.255.0.0

access-list to_hono1 permit ip 192.168.0.0 255.255.0.0 10.2.0.0 255.255.0.0

access-list to_hono2 permit ip 172.16.0.0 255.255.0.0 10.2.0.0 255.255.0.0

crypto map vpn_tunnel 1 ipsec-isakmp

crypto map vpn_tunnel 1 match address to_anchor1

crypto map vpn_tunnel 1 set peer 16.16.8.2

crypto map vpn_tunnel 1 set transform-set vpnHolly

crypto map vpn_tunnel 2 ipsec-isakmp

crypto map vpn_tunnel 2 match address to_anchor2

crypto map vpn_tunnel 2 set peer 16.16.8.2

crypto map vpn_tunnel 2 set transform-set vpnHolly

```
crypto map vpn_tunnel 3 ipsec-isakmp
crypto map vpn_tunnel 3 match address to_hono1
crypto map vpn_tunnel 3 set peer 16.16.8.3
crypto map vpn_tunnel 3 set transform-set vpnHolly
crypto map vpn_tunnel 4 ipsec-isakmp
crypto map vpn_tunnel 4 match address to_hono2
crypto map vpn_tunnel 4 set peer 16.16.8.3
crypto map vpn_tunnel 4 set transform-set vpnHolly
crypto map vpn_tunnel interface outside
access-list no_nat permit ip 172.16.0.0 255.255.0.0 10.0.0.0 255.0.0.0
access-list no_nat permit ip 192.168.0.0 255.255.0.0 10.0.0.0 255.0.0.0
nat (inside) 0 access-list no_nat
sysopt connection permit-ipsec
```

Laboratory Practice #4

This practice requires the instructor to erase any previous Phone configuration parameters and Voice VLANs descriptions from previous implementation in the routers. The routers and their networks must be able to communicate so a minimum basic configuration with NAT is needed. The following are things that the instructor needs to consider before the practice.

1. Reset the IP Phones before the practice by entering accessing the Settings Menu and pressing **#**
2. Save the configuration of the routers and reload them to avoid any error during the creation of the CNF files.

Router ANCHORAGE Preliminary Configuration Commands

vlan 2

no name

vlan 3

no name

vlan 4

no name

vlan 5

no name

Router HONOLULU Preliminary Configuration Commands

vlan 2

no name

vlan 3

no name

vlan 4

no name

vlan 5

no name

During the implementation of the practice commands, it is important to consider that the clock set command needs to be adjusted to reflect the actual time of the implementation. The MAC addresses of the ephone configuration don't necessarily need to follow the order presented here. The command no create cnf-files will not work if there are no cnf-files, this doesn't affect the Laboratory Practice in any way.

Router ANCHORAGE Practice Commands

```
vtp mode transparent
vlan 2
name DATA
interface vlan 2
description Data_Services
vlan 3
name VOICE
interface vlan3
description Telephone_Services
ip address 10.1.64.1 255.255.192.0
no shutdown
interface range fastEthernet 0/1/0 - 3
switchport mode access
switchport access vlan 2
switchport voice vlan 3
auto qos voip trust
ip dhcp excluded-address 10.1.0.1
ip dhcp excluded-address 10.1.64.1
ip dhcp pool PC_DEV
network 10.1.0.0 255.255.192.0
default-router 10.1.0.1
dns-server 172.16.0.2
```

```
exit
ip dhcp pool PH_DEV
network 10.1.64.0 255.255.192.0
default-router 10.1.64.1
option 150 ip 10.1.64.1
exit
clock timezone CST -6
do clock set 21:15:00 april 13 2011
telephony-service
max-ephones 4
max-dn 4
ephone-dn 1
number 1001
exit
ephone-dn 2
number 1011
exit
ephone 1
mac-address 0021.5503.419b
button 1:1
exit
ephone 2
mac-address 0021.5554.9d4e
```

button 1:2

exit

telephony-service

ip source-address 10.1.64.1

no create cnf-files

create cnf-files

dial-peer voice 1 voip

destination-pattern 2...

session target ipv4:16.16.8.3

Router HONOLULU Practice Commands

vtp mode transparent

vlan 2

name DATA

interface vlan 2

description Data_Services

vlan 3

name VOICE

interface vlan 3

description Telephone_Services

ip address 10.2.64.1 255.255.192.0

no shutdown

interface range fastEthernet 0/1/0 - 3

switchport mode access

```
switchport access vlan 2
switchport voice vlan 3
auto qos voip trust
ip dhcp excluded-address 10.2.0.1
ip dhcp excluded-address 10.2.64.1
ip dhcp pool PC_DEV
network 10.2.0.0 255.255.192.0
default-router 10.2.0.1
dns-server 172.16.0.2
exit
ip dhcp pool PH_DEV
network 10.2.64.0 255.255.192.0
default-router 10.2.64.1
option 150 ip 10.2.64.1
exit
clock timezone CST -6
do clock set 21:15:00 april 13 2011
telephony-service
max-ephones 4
max-dn 4
ephone-dn 1
number 2001
exit
```

ephone-dn 2

number 2011

exit

ephone 1

mac-address 0021.5503.419b

button 1:1

exit

ephone 2

mac-address 0021.5554.9d4e

button 1:2

exit

telephony-service

ip source-address 10.2.64.1

no create cnf-files

create cnf-files

dial-peer voice 1 voip

destination-pattern 1...

session target ipv4:16.16.8.2

Laboratory Practice #5

This practice requires a basic routing and VPN implementation between the Cisco 2800 Series routers and the firewall. So the configuration of Laboratory Practice #3 must have been implemented prior to this practice. This laboratory practice doesn't have any

commands to be entered in the routers prior to its implementation. The instructor will need to verify the following:

1. Verify that the VPN connection between the sites is working and that the Server is properly running.
2. The Wireless interface (Network Connection) in Host Anchorage and Host Honolulu is active and the REALTEK Wireless LAN Utility must be working.
3. The local area connection (Ethernet connection) in Host Anchorage and Host Honolulu must be deactivated to avoid any conflict. The instructor might unplug the cables if considered necessary.

The commands to be implemented during the practice are the following:

Router ANCHORAGE Practice Commands

```
vlan 4
name WLAN1
no shutdown
exit
vlan 5
name WLAN2
no shutdown
exit
dot11 ssid Employees_A
vlan 4
 guest-mode
exit
```

```
dot11 ssid Management_A
vlan 5
exit
interface dot11radio0/3/0
channel least-congested
exit
interface dot11radio0/3/0.4
encapsulation dot1q 4
description wireless01
ip address 10.1.128.1 255.255.224.0
ip nat inside
exit
interface dot11radio0/3/0.5
encapsulation dot1q 5
description wireless02
ip address 10.1.160.1 255.255.224.0
ip nat inside
exit
ip dhcp excluded-address 10.1.128.1
ip dhcp excluded-address 10.1.160.1
ip dhcp pool WIRELESS1
network 10.1.128.0 255.255.224.0
default-router 10.1.128.1
```

```
dns-server 172.16.0.2
exit
ip dhcp pool WIRELESS2
network 10.1.160.0 255.255.224.0
default-router 10.1.160.1
dns-server 172.16.0.2
exit
interface dot11radio0/3/0
ssid Employees_A
ssid Management_A
antenna receive diversity
antenna transmit diversity
no shutdown
interface dot11radio0/3/0
encryption vlan 4 mode ciphers tkip
encryption vlan 5 mode ciphers tkip
exit
dot11 ssid Employees_A
authentication open
 authentication key-management wpa
wpa-psk ascii anem4411
exit
dot11 ssid Management_A
```

authentication open

authentication key-management wpa

wpa-psk ascii anma4411

exit

Router HONOLULU Practice Commands

vlan 4

name WLAN1

no shutdown

exit

vlan 5

name WLAN2

no shutdown

exit

dot11 ssid Employees_H

vlan 4

guest-mode

exit

dot11 ssid Management_H

vlan 5

exit

interface dot11radio0/3/0

channel least-congested

exit

```
interface dot11radio0/3/0.4
encapsulation dot1q 4
description wireless01
ip address 10.2.128.1 255.255.224.0
ip nat inside
exit
interface dot11radio0/3/0.5
encapsulation dot1q 5
description wireless02
ip address 10.2.160.1 255.255.224.0
ip nat inside
exit
ip dhcp excluded-address 10.2.128.1
ip dhcp excluded-address 10.2.160.1
ip dhcp pool WIRELESS1
network 10.2.128.0 255.255.224.0
default-router 10.2.128.1
dns-server 172.16.0.2
exit
ip dhcp pool WIRELESS2
network 10.2.160.0 255.255.224.0
default-router 10.2.160.1
dns-server 172.16.0.2
```

```
exit
interface dot11radio0/3/0
ssid Employees_H
ssid Management_H
antenna receive diversity
antenna transmit diversity
 no shutdown
interface dot11radio0/3/0
encryption vlan 4 mode ciphers tkip
encryption vlan 5 mode ciphers tkip
exit
dot11 ssid Employees_H
authentication open
 authentication key-management wpa
wpa-psk ascii hoem4411
exit
dot11 ssid Management_H
 authentication open
authentication key-management wpa
wpa-psk ascii homa4411
exit
```

Laboratory Practice #6

This practice requires a previous successful implementation of Laboratory Practice #3. This practice uses the HOLLYWOOD02 firewall. The instructor needs to verify the following:

1. The Cisco VPN Client has been installed in at least one computer. The VPN Client can be downloaded from the ITS website. Any connection entry must be deleted.
2. The server must be working and there must be connectivity within the internal network.

Firewall HOLLYWOOD02 Practice Commands

```
crypto ipsec transform-set r_c_vpn esp-3des esp-sha-hmac
crypto dynamic-map remote_client 10 set transform-set r_c_vpn
crypto map vpn_tunnel 99 ipsec-isakmp dynamic remote_client
crypto map vpn_tunnel interface outside
access-list no_nat permit ip 172.16.0.0 255.255.0.0 172.16.0.0 255.255.255.0
access-list no_nat permit ip 192.168.0.0 255.255.0.0 172.16.0.0 255.255.255.0
ip local pool RAPOOL 172.16.0.129-172.16.0.254 mask 255.255.255.0
isakmp client configuration address-pool local RAPOOL outside
crypto map vpn_tunnel client configuration address initiate
no isakmp key vpnkey4411 address 16.16.8.2
no isakmp key vpnkey4411 address 16.16.8.3
isakmp key vpnkey4411 address 16.16.8.2 no-xauth no-config-mode
isakmp key vpnkey4411 address 16.16.8.3 no-xauth no-config-mode
aaa-server LOCAL protocol local
```

username administrator password cisc4411 privilege 15

username testvpn password acc4411 privilege 2

crypto map vpn_tunnel client authentication LOCAL

vpngroup REMUSERS password 4411class

vpngroup REMUSERS dns-server 172.16.0.2

vpngroup REMUSERS default-domain cerveau.com

Laboratory Practice #7

A RADIUS Server must be properly running for the implementation of Laboratory Practice #6. The students will be using the NTRadPing test utility which will need to be installed in the Anchorage Host and the Honolulu Host. It is important to remember that any modification to the RADIUS database will require the service to be restarted. The instructor will need to perform the following tasks prior to the implementation of the practice.

1. Verify that the Anchorage and Honolulu networks can reach the RADIUS Server.
2. Verify that the graphical interface Dial-UP Admin is working.
3. Verify that users, clients and groups can be created in the RADIUS Server.
4. Verify that the NTRadPing test utility is properly working.
5. Delete all users, clients, and groups from the RADIUS database and restart the service.

Since this practice is focused entirely in the RADIUS Server, there are no commands to be implemented.

Laboratory Practice #8

Prior to the implementation of this practice, it is necessary for the Cisco 2800 Series Routers and the Perimeter Firewall to have a working VPN connection. In addition, laboratory practice #5, #6 and #7 must have been implemented before this practice since wireless services, remote-access VPN, and the RADIUS' users, group and clients are needed for the proper implementation of RADIUS in the different network devices. The instructor will have to perform the following activities before the practice:

1. Prepare an external host with the Cisco VPN client properly configured and working.
2. Verify that the Anchorage and Honolulu networks can reach the RADIUS Server.
3. Verify that the users, client and groups were properly introduced in the RADIUS Server database and that the RADIUS server is working.
4. Verify that the Wireless Networks for both Anchorage and Honolulu are working.

Firewall HOLLYWOOD02 Practice Commands

no username administrator

no username testvpn

no crypto map vpn_tunnel client authentication LOCAL

aaa-server RADIUS protocol radius

aaa-server RADIUS (inside) host 172.16.0.2 radcl4411

crypto map vpn_tunnel client authentication RADIUS

aaa-server radius-authport 1812

Router ANCHORAGE Practice Commands

dot11 ssid Management_A

no wpa-psk

no authentication key-management wpa

aaa new-model

radius-server host 172.16.0.2 auth-port 1812 acct-port 1813 key radcl4411

ip radius source-interface dot11Radio 0/3/0.4

aaa authentication login wireless_eap group radius

dot11 ssid Management_A

authentication open eap wireless_eap

authentication network-eap wireless_eap

interface Dot11Radio0/3/0

encryption vlan 5 mode ciphers tkip aes-ccm wep128

Router HONOLULU Practice Commands

dot11 ssid Management_H

no wpa-psk

no authentication key-management wpa

aaa new-model

radius-server host 172.16.0.2 auth-port 1812 acct-port 1813 key radcl4411

ip radius source-interface dot11Radio 0/3/0.4

aaa authentication login wireless_eap group radius

dot11 ssid Management_H

authentication open eap wireless_eap

authentication network-eap wireless_eap

interface Dot11Radio0/3/0

encryption vlan 5 mode ciphers tkip aes-ccm wep128

APPENDIX F

LABORATORY PRACTICES

LABORATORY PRACTICE #1

IMPLEMENTING A DEMILITARIZED ZONE (DMZ)

Objectives

By completing this laboratory practice the student will be able to:

1. Configure the necessary parameters on PIX firewalls to set up a basic DMZ layout.
2. Configure Access Control Lists (ACLs) based on communication protocols.
3. Perform basic troubleshooting of communication issues between segments of a network.

Introduction

Cerveau Inc. is a financial services company, headquartered in Los Angeles CA, with many branches through the nation. You have been recently hired as a Network Administrator in charge of protecting and managing the corporate network. The company needs to provide services such as Mail (SMTP), DHCP, and DNS to clients in the internal network, with the prospect of extending these services to other clients through VPN connections. Web services on the other hand, need to be available outside the network to people that need to access the company website from the internet. ICMP will be allowed for testing purposes. The company has two servers intended to provide different services for the company. These servers need to be accessible for both internal and external users under a DMZ scheme. Currently two PIX firewalls are available to design a solution that will secure the DMZ where the servers will be located. The following addressing scheme will be used:

Internal Network:	Networks 192.168.240.0, divided in subnets with /30 mask for links.
	Networks 192.168.1.0 to 192.168.10.0 /24, will be used by hosts.
DMZ Network:	Networks 172.16.0.0, Subnet 0 with /24 will be used.
Public Addresses:	16.16.8.1 and 16.16.8.2.

PART I

INTRODUCTION TO FIREWALLS AND DMZ

Firewalls are intended to secure segments of a computer network by denying specific types of network traffic or hosts, based on the security policies defined by the network administrator. Firewalls can take different forms, from software inside a PC or server to hardware solely dedicated to filtering traffic.

One basic form of firewall solution is a single router or other firewall device in the perimeter of the network, known as perimeter firewall, which will implement traffic filtering policies or ACLs. This is usually seen in small computer networks but might not be adequate for networks that offer public services. A more secure firewall solution can be achieved by using a dedicated firewall, known as internal firewall, between the perimeter firewall and the internal network. This creates a third network between the two firewalls, the demilitarized zone (DMZ), which can be used to allocate the computer servers that provide public services to both the internal and external networks. The following sections present the necessary guidelines to implement an example of this solution as presented in Figure 1.

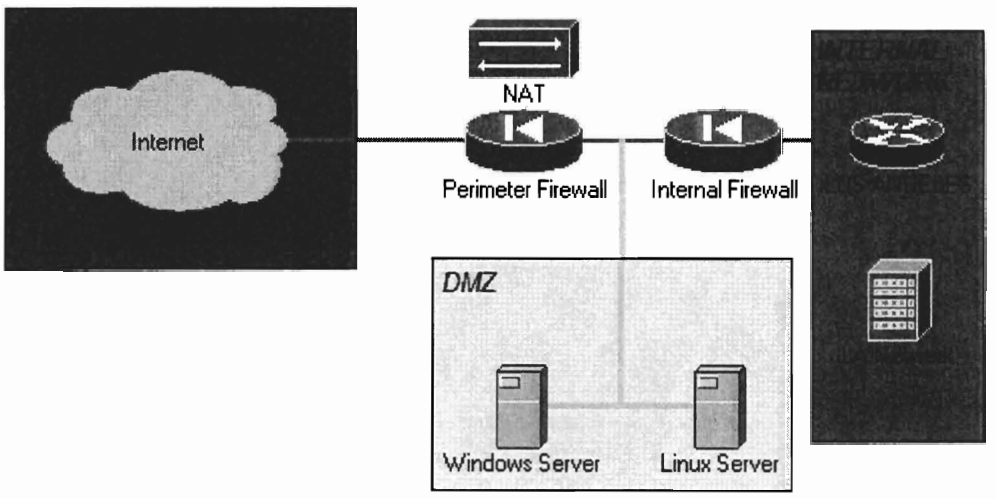


Figure 1. Desired DMZ layout including affected networks.

The perimeter firewall works as the first line of defense against any type of attack, isolating the external network from both the DMZ and the internal network, while the internal firewall separates the DMZ from the internal network, adding a second layer of defense against external attackers.

The firewalls used in the laboratory have two Ethernet interfaces that filter traffic based on a security level scheme. The interface *Ethernet 0*, labeled as *Outside* Interface has a security level of 0; while the interface *Ethernet 1*, labeled as *Inside* Interface has a security level of 100. The security levels define the usual behavior of firewalls: by default, traffic will flow freely from a high-security level segment to a low-security level segment, while the traffic flowing between segments of the same security level and from lower to higher security levels will be regulated.

Complete Part A of the Activity review sheet.

PART II

BASIC FIREWALL CONFIGURATION

The firewalls will be configured from scratch. The Firewall's command line interface (CLI) shares some similarities with its router counterpart; nevertheless, most of the commands syntax and the data's presentation are significantly different, which requires an examination of the basic configuration. Anchorage and Honolulu consoles will be used for the configuration.

Step 1: Accessing the console and reviewing the available modes.

The *exec mode* of a firewall is similar to a router in the sense that it can be identified by the > symbol in the CLI prompt as followss: Pixfirewall>

Entering the command *enable* and introducing the password will change the CLI prompt to *privileged exec mode* as followss: Pixfirewall#

The configuration mode will be accessed with the command *configure terminal.* The CLI prompt changes as followss: Pixfirewall(config)#

Step 2: Erasing the firewall configuration.

The command *write erase* erases the starting configuration of the firewall and initializes the fabric default configuration the next time the firewall is restarted. The procedure is as follows:

Pixfirewall#write erase

Pixfirewall#reload

After the *write erase* command, the firewall will ask for a confirmation. During the reload process the firewall will show the model of the device, record the model for future use. Before launching the CLI the firewall will ask if the user wants to enter an interactive configuration prompt, it is necessary to enter the letter "*n*" in order to return to the *exec mode.*

Step 3: Providing a name for the firewall.

This is done from the configuration mode. In order to establish a name for the device the command *hostname* is used as follows:

Pixfirewall(config)#hostname HOLLYWOOD01 (*If you are using the PIX 506E*)

Pixfirewall(config)#hostname HOLLYWOOD02 (*If you are using the PIX 501*)

From this point onward each firewall will be referred by its name.

Step 4: Defining a password for the *privileged exec* mode.

In both cases, the password will be set to class. This is done by using the command *enable password* in the configuration mode as follows:

Firewall HOLLYWOOD01:

HOLLYWOOD01(config)#enable password class

Firewall HOLLYWOOD02:

HOLLYWOOD02(config)# enable password class

Step 5: Activating the firewall interfaces.

By default, the interfaces of the firewall are deactivated, in order to activate an interface it is necessary to define a speed. This is done as follows:

Firewall HOLLYWOOD01:

HOLLYWOOD01(config)#interface ethernet0 auto

HOLLYWOOD01(config)#interface ethernet1 auto

Firewall HOLLYWOOD02:

HOLLYWOOD02(config)#interface ethernet0 100full

HOLLYWOOD02(config)#interface ethernet1 100full

PIX firewalls don't have a submenu for interface settings. For this scenario the speed for HOLLYWOOD01 was set to AUTO, indicating that it will negotiate the transmission speed with its neighbor. The speed for HOLLYWOOD02 was set to 100Kbps Full Duplex.

Step 6: Assigning ip addresses to the interfaces.

As previously explained, the firewall assigns names and security levels to the interfaces by default: *Outside* and security level 0 to interface *ethernet0*; and *inside* with security level 100 to interface ethernet1.

Firewall HOLLYWOOD01:

HOLLYWOOD01(config)#ip address inside 192.168.240.26 255.255.255.252

HOLLYWOOD01(config)#ip address outside 172.16.0.1 255.255.255.0

Firewall HOLLYWOOD02:

HOLLYWOOD02(config)#ip address inside 172.16.0.126 255.255.255.0

HOLLYWOOD02(config)#ip address outside 16.16.8.1 255.255.255.0

Figure 2 presents a diagram of the inside and outside networks from the context of both firewalls: The inside network for HOLLYWOOD01 corresponds to the link between LOS_ANGELES and the Firewall with the address 192.168.240.26/30 assigned to the *inside interface*. The DMZ network corresponds to HOLLYWOOD02 inside network and to HOLLYWOOD01 outside network; with the first available address of the segment 172.16.0.0/24 assigned to HOLLYWOOD01 and the address 172.16.0.126 assigned to HOLLYWOOD02. The external network presented in Figure 1 corresponds to the Outside network of HOLLYWOOD02 which was assigned the public address of 16.16.8.1 and covers any network that doesn't belong to the company.

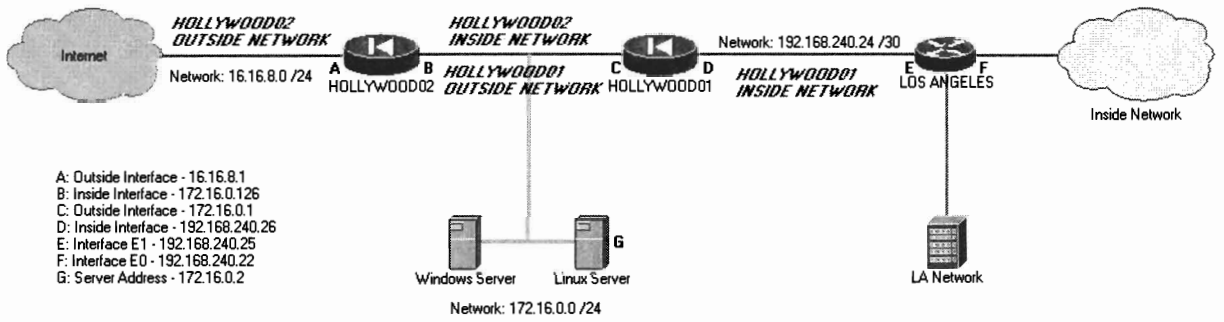


Figure 2. Outside and Inside networks from the firewalls' standpoint.

Step 7: Establish static routes for the firewalls.

Routes for the different networks need to be created in the firewalls in order to establish communication between the different networks. Both firewalls have the DMZ network directly connected and the routing within the DMZ is performed by the Linux Server. The routes that need to be defined are the routes that are not directly connected to the firewalls and any default route, this is done as follows:

Firewall HOLLYWOOD01:

HOLLYWOOD01(config)#route inside 192.168.0.0 255.255.0.0 192.168.240.25 1

HOLLYWOOD01(config)#route outside 0.0.0.0 0.0.0.0 172.16.0.126 1

Firewall HOLLYWOOD02:

HOLLYWOOD02(config)#route inside 192.168.0.0 255.255.0.0 172.16.0.1 1

HOLLYWOOD02(config)#route outside 0.0.0.0 0.0.0.0 16.16.8.2 1

Both HOLLYWOOD01 and HOLLYWOOD02 route packages addresses to the internal network by using address summarization, comprising all the networks in the 192.168.0.0 segment in a single route that points to the next hop. Notice that both firewalls have a default route for any external address not defined in their routing table.

Step 8: Deactivating Network Address Translation (NAT) in the Internal Firewall.

A particularity of PIX firewalls is that by default it is assumed that NAT will exist between the *inside* interface and the *outside* interface. NAT for the networks that belong to the company is not needed, so in the case of HOLLYWOOD01, it is necessary to disable NAT in the inside interface by using the following procedure:

Firewall HOLLYWOOD01:

HOLLYWOOD01(config)#access-list NO_NAT_NEEDED permit ip any any

HOLLYWOOD01(config)#nat (inside) 0 access-list NO_NAT_NEEDED

The first command specifies the ACL, in this case any host address going to any network will be allowed to pass without being translated, the second command bounds the ACL to the inside interface.

Since firewalls block traffic from a lower security level to a higher security level the existence of a route to a network allows any connections from the internal clients to the DMZ and external network but not the other way around. To control the traffic allowed, the creation of ACLs becomes necessary.

Complete Part B of the Activity review sheet.

PART III

CONFIGURING ACLs IN THE PIX FIREWALL

This section explains how to establish access policies in the form of ACLs to filter and control traffic for the external network, the DMZ and the internal network. ACLs can be either standard or extended: Standard ACLs can be used to filter general traffic coming from specific networks or hosts; extended ACLs, allow filtering of specific protocols or applications, granting a greater control over the flow of traffic. In this particular scenario, an access policy based on the requirements of the internal and external clients has been established. The requirements include the following services that will be provided by the DMZ to the internal clients: DHCP, DNS, FTP and access to the web server. External clients must be able to access the web server and nothing more while internal clients must be able to leave the network just for web browsing and ping. Any type of traffic that doesn't match with the access policy will be restricted.

Step 1: Allowing ICMP Traffic for testing.

For testing purposes ICMP traffic will be allowed for traffic flowing through all networks, by doing this, users will be able to ping sites and clients outside the internal network, this is accomplished with the following ACLs:

Firewall HOLLYWOOD01:

HOLLYWOOD01(config)#access-list INCOMING permit icmp any any

HOLLYWOOD01(config)#access-list OUTGOING permit icmp any any

Firewall HOLLYWOOD02:

HOLLYWOOD02(config)#access-list INCOMING permit icmp any any

HOLLYWOOD02(config)#access-list OUTGOING permit icmp any any

The names *INCOMING* and *OUTGOING* are assigned arbitrary by the network administrator. In this case they specify the traffic that is allowed to enter and leave the network. As Figure 3 indicates, by default the outgoing traffic is allowed in the firewalls, this might raise different security concerns in the form of internal attackers compromising the network. The *permit* statement indicates that the traffic specified as ICMP will be allowed. The first *any* refers to the ip addresses that initiate the traffic, in this case any ip address will be allowed, while the second *any* refers to the destination ip addresses.

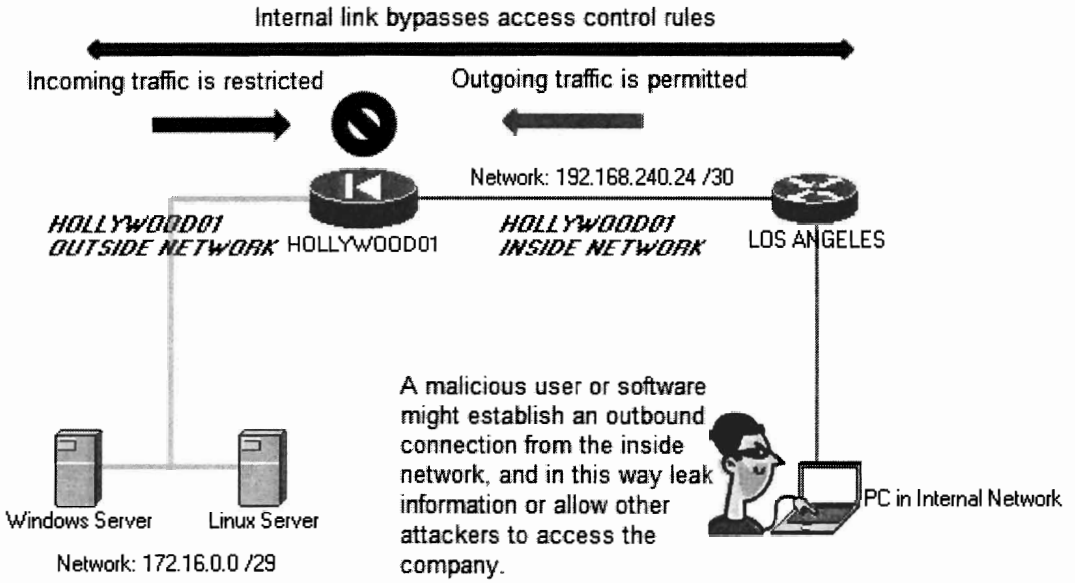


Figure 3. Security concerns associated with default firewall configuration.

Step 2: Allowing web browsing traffic.

Web browsing traffic will be allowed for both the internal network and the DMZ and together with ICMP will be the only traffic allowed to reach the external network. This is done as follows:

Firewall HOLLYWOOD01:

HOLLYWOOD01(config)#access-list OUTGOING permit tcp any any eq www

Firewall HOLLYWOOD02:

HOLLYWOOD02(config)#access-list OUTGOING permit tcp any any eq www

HOLLYWOOD02(config)#access-list INCOMING permit tcp any any eq www

Notice the differences between the web traffic ACL statement and the ICMP ACL: The *permit* statement allows *tcp* traffic from *any* source to *any* destination as long as it's marked using the www port, which specifies the service provided is web browsing. HOLLYWOOD02 has an extra line allowing incoming web traffic; this is done in order for external users to access the website.

Step 3: Allowing FTP traffic between the DMZ and the internal network.

FTP can work in both passive and active mode. The current scenario presents the configuration to allow passive FTP traffic between the internal network and the DMZ:

Firewall HOLLYWOOD01:

HOLLYWOOD01(config)#access-list OUTGOING permit tcp any host 172.16.0.2 eq ftp

HOLLYWOOD01(config)#access-list OUTGOING permit tcp any host 172.16.0.2 range 1024 1030

Notice the difference between this ACL and the previous ACLs: Traffic is specified as *tcp* coming from *any* source and going specifically to the FTP server address; *eq ftp* defines the

port used for FTP while *range 1024 1030* indicates that any port within the range of 1024 and 1030 (included) will be allowed. Passive FTP uses any port higher than 1024 to establish the data communication link.

Step 4: Allowing DHCP traffic between the DMZ and the internal network.

DHCP uses two *udp* ports: One for server transmissions and one for client transmissions. The following ACLs allow DHCP traffic to automatically assign IP addresses:

Firewall HOLLYWOOD01:

HOLLYWOOD01(config)#access-list INCOMING permit udp host 172.16.0.2 eq bootps any

HOLLYWOOD01(config)#access-list OUTGOING permit udp any eq bootpc host 172.16.0.2

Notice that the first ACL refers to incoming traffic from the DHCP server masked as 172.16.0.2 and going to *any* internal host by using the bootps port which indicates that is server traffic. The second ACL allows *any* internal host sending a DHCP request to contact the DHCP server.

Step 5: Allowing DNS traffic between the DMZ and the internal network.

DNS allows the translation of names to ip addresses, which is done by using both *udp* and *tcp* ports. The following ACLs permit the DNS traffic:

Firewall HOLLYWOOD01:

HOLLYWOOD01(config)#access-list OUTGOING permit udp any eq domain any

HOLLYWOOD01(config)#access-list OUTGOING permit udp any any eq domain

HOLLYWOOD01(config)#access-list OUTGOING permit tcp any eq domain any

HOLLYWOOD01(config)#access-list OUTGOING permit tcp any any eq domain

Notice that in both *udp* and *tcp* cases, the incoming traffic and the outgoing traffic using the domain port is controlled separately and not in the same ACL.

Step 6: Denying traffic that doesn't match with policies and associating interfaces.

After specifying the traffic to be permitted in both firewalls it is important to deny the rest of the traffic. The outside interface does this by default, but the inside interface is set to allow all traffic, so it is important to restrict the traffic leaving this interface. Finally, the ACLs need to be associated with an interface in order to ba activated in the firewall; this is done with the following procedure:

Firewall HOLLYWOOD01:

HOLLYWOOD01(config)#access-list INCOMING deny ip any any

HOLLYWOOD01(config)#access-list OUTGOING deny ip any any

HOLLYWOOD01(config)#access-group INCOMING in interface outside

HOLLYWOOD01(config)#access-group OUTGOING in interface inside

Firewall HOLLYWOOD02:

HOLLYWOOD02(config)#access-list INCOMING deny ip any any

HOLLYWOOD02(config)#access-list OUTGOING deny ip any any

HOLLYWOOD02(config)#access-group INCOMING in interface outside

HOLLYWOOD02(config)#access-group OUTGOING in interface inside

Notice the *ip* statement: It indicates that any traffic being ip in nature, either tcp, udp or icmp is affected by the clause. The *deny* statement indicates that traffic is being denied.

Step 7: Configuring NAT in the perimeter firewall.

In order for the internal hosts to reach the outside network it's necessary to translate their private addresses into public addresses. This is done by means of NAT. Details concerning NAT will be explained in future practices. For this scenario one address will translate all the hosts in

the network while one address will be used exclusively for the Linux server. This is done as follow:

Firewall HOLLYWOOD02:

HOLLYWOOD02(config)#global (outside) 1 interface

HOLLYWOOD02(config)#nat (inside) 1 0.0.0.0 0.0.0.0 0 0

HOLLYWOOD02(config)# static (inside, outside) 16.16.8.4 172.16.0.2

Complete Part C of the Activity review sheet.

LABORATORY PRACTICE #1

ACTIVITY REVIEW SHEET

The following are different tasks to be completed by the end of each section of the laboratory guide. Ask the instructor if there is any problem completing any activity.

PART A

1. Access a host specified by the instructor. Enter the command line and use the command *ipconfig /all*. Record the following information:

   IP address/Mask: _____

   Default Gateway/Router: _____

   Is DHCP enabled? _____ Address of the DHCP server: _____

   DNS Servers addresses: _____

   Lease expiration date: _____

2. Ping the following public address: 16.16.8.8. Was the ping successful? _____
3. Open a web browser and enter the following address: www.cerveau.com. Was the website displayed? _____
4. Access the ftp server option from the website. List any file stored in the ftp server:

   _____

Complete Part II of the Laboratory Guide.

PART B

1. From the firewall. Verify the interface status in the firewall with the commands *show interface*.

   Firewall(config)#show interface ethernet0

   Firewall(config)#show interface ethernet1

Are the interfaces and line protocol up? _____

Notice the difference between the display of this command from the firewall and a router.

2. Use the *show running-config* to display the whole firewall configuration. Notice the difference between the display of the firewall and a router. The lines marked as nameif indicate the name assigned to the interfaces and the security levels.

   Record the names assigned by the firewall to the interface.

   Interface Ethernet 0:_____

   Interface Ethernet 1:_____

   Record the security levels of both interfaces:

   Interface Ethernet 0:_____

   Interface Ethernet 1:_____

3. Use the *show route* command to display the assigned and automatically created routes in the firewall. Routes marked as CONNECT are directly connected routes, record them and compare them with the routes that you defined.

   _____

   _____

4. Access the host previously specified by the instructor. Manually assign the ip address, mask and DNS servers specified in part A. Ping the HOLLYWOOD01 inside interface as follow: ping 192.168.240.26. Was the ping successful? _____
5. From the host, ping the dhcp server specified in part A. Was the ping successful? _____
6. From the host, ping the public address specified in part A. Was the ping successful? _____
7. Open a web browser and enter the following url: www.cerveau.com. Was the website displayed? _____

8. Configure the host to automatically obtain an ip address. Was the address obtained successfully? _____

Notice that communications in the form of web browsing and DNS resolve are possible but DHCP cannot be assigned and ping doesn't respond. This is because both DHCP and ICMP require an answer that is send by the server in the outside interface of the Internal Firewall and traffic from a lower to a higher security level is not allowed by default.

Complete Part III of the Laboratory Guide.

PART C

1. Configure the host specified by the instructor to automatically obtain an IP address. Was the address obtained successfully? ___
2. Access the external host 16.16.8.8. Enter the following url in a web browser: www.cerveau.com. Was the operation successful? _____ Why?

   _____

   _____
3. Enter the address: 16.16.8.4 in the web browser. Was the operation successful? _____ Why?

   _____

   _____
4. Try to access ftp services from the external host. Was the operation successful?_____

LABORATORY PRACTICE #2

NETWORK AND PORT ADDRESS TRANSLATION (NAT & PAT)

Objectives

By completing this laboratory practice the student will be able to:

1. Define groups of hosts that will participate in the NAT process.
2. Establish a pool of addresses for NAT purposes.
3. Configure NAT in routers and firewalls.
4. Configure PAT in routers and firewalls.
5. Troubleshoot and verify typical NAT and PAT configuration.

Introduction

Cerveau Inc., which recently hired you as a network administrator, has opened new branches in the cities of Honolulu and Anchorage. You have been assigned with the task of establishing access for these branches to the external network as well as defining the NAT/PAT configuration for the corporate/internal network to provide Internet access to all hosts in the network and to allow the Multipurpose server to be accessible from the External network. The following public addresses have been assigned to the company in order to establish NAT/PAT:

1. 16.16.8.1, for both the Perimeter and Internal Network.
2. 16.16.8.2, for the Anchorage Branch.
3. 16.16.8.3, for the Honolulu Branch.
4. 16.16.8.4, for the multipurpose Server.

To verify that NAT and PAT have been set up properly, the computers in the corporate network and in the networks of Anchorage and Honolulu should be able to ping the TESTING PC (Address 16.16.8.8) by using the ping function.

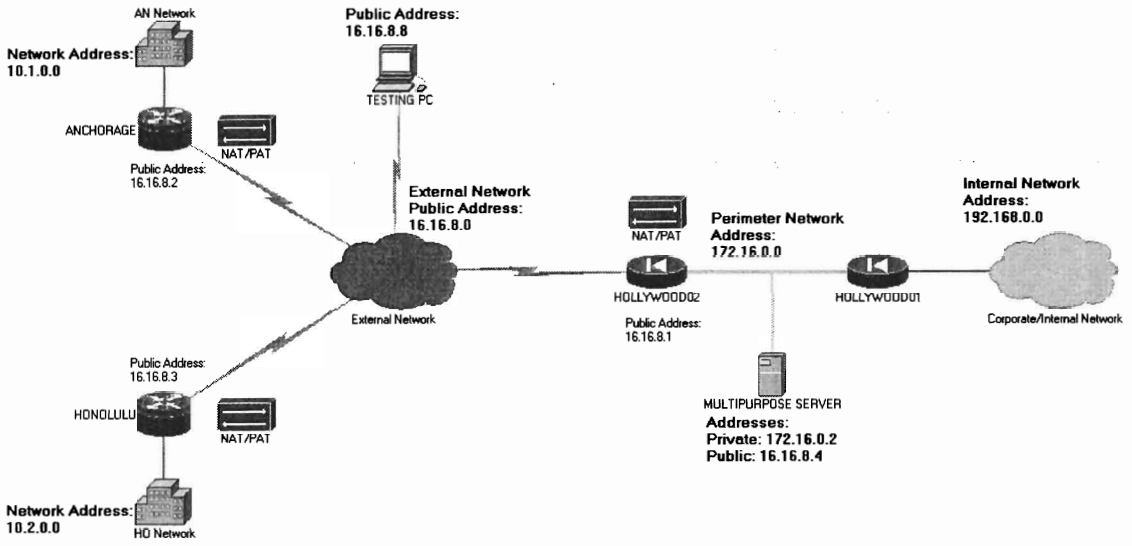


Figure 1. Network layout for Cerveau Inc.

PART I

BASIC CONCEPTS OF NAT AND PAT

The main use of NAT and PAT is to address the issue concerning the shortage of IPv4 address. Since more and more companies need access to the Internet, the Internet Engineering Task Force (IETF) established a set of private addresses that can be used by the different companies inside their networks, while public addresses where used in the Internet. Due to their nature, these private addresses cannot be forwarded to a public network, since more than one host in different companies might be using the same private address. It is for this reason that NAT and PAT become necessary. In this case, the private networks that have to be translated are the following:

1. Network 10.1.0.0 for ANCHORAGE.
2. Network 10.2.0.0 for HONOLULU.
3. Network 172.16.0.0 and 192.168.0.0 for the Perimeter and Corporate Network.

NAT and PAT can hide the actual address of resources in the internal network from external users, and by doing this, work as an additional security mechanism. The addresses being subject to translation in the network are referred as the ***inside local addresses***; while the addresses that are defined in a pool and that will be available for translation purposes are known as the ***inside global addresses***. In regards to a destination located in the external network, the address that it uses for its hosts are known as ***outside local addresses***; while the public addresses that are used as the translation are known as ***outside global addresses***; in both cases is outside, since these addresses are outside our network.

The difference between NAT and PAT is that while NAT assigns a single local address to a global address in a one to one relation, PAT uses ports to assign multiple local addresses to one ore many global addresses; the procedure is basically the same, which gives PAT the name of NAT overloaded.

Complete Part A of the Activity review sheet.

PART II

CONFIGURING PAT

Step 1: Defining the pools of global addresses.

In the case of the routers, there are a few things that need to be considered; the syntax of the command to define a pool of global addresses is as follow: **ip nat pool** ***name start_address end_address*** **netmask** ***mask***. In this case, since there is only one ip address for the routers, the start address will be the same end address.

Router ANCHORAGE:

ANCHORAGE(config)# ip nat pool a_nat 16.16.8.2 16.16.8.2 netmask 255.255.255.0

Router HONOLULU:

HONOLULU(config)# ip nat pool h_nat 16.16.8.3 16.16.8.3 netmask 255.255.255.0

In the case of the firewall, it is necessary to consider that the server located in the perimeter network has to be accessible from the outside network. This issue will need to be addressed latter by means of static NAT configuration. For the rest of the networks, a dynamic configuration will be used, which will require the definition of a pool, this is done as follow:

Firewall HOLLYWOOD02:

HOLLYWOOD02(config)#global (outside) 1 interface

Notice that the command is considerably different from the router; in this case the syntax is as follow: **global (*logical_interface_name*) *pool_number start_address end_address* netmask *mask***. The first thing to consider is that the pool doesn't get a name but a number; and that is necessary to specify the interface in which the address will be translated (outside, in thiscase), the start address and end address have been substituted in this case for the statement **interface**, indicating that we are taking the ip address and mask from the ***outside*** interface.

Step 2: Defining the inside addresses to be translated.

This is done in the routers by means of a simple ACL, as follow:

Router ANCHORAGE:

ANCHORAGE(config)# access-list 1 permit 10.1.0.0 0.0.255.255

Router HONOLULU:

HONOLULU(config)# access-list 1 permit 10.2.0.0 0.0.255.255

In the case of the firewall, the following command specifies the addresses to be translated:

Firewall HOLLYWOOD02:

HOLLYWOOD02(config)#nat (inside) 1 0.0.0.0 0.0.0.0 0 0

The zeros indicate that all the internal addresses will be translated. The ***nat*** command not only specifies the addresses to translate but activates NAT/PAT in the firewall. In order to activate PAT for the routers two extra steps are needed.

Step 3: Establishing the dynamic translation of the addresses.

The internal addresses in the routers have will be associated with the NAT pools, it is necessary to specify the **overload** statement, this is done as follow:

Router ANCHORAGE:

ANCHORAGE(config)# ip nat inside source list 1 pool a_nat overload

Router HONOLULU:

HONOLULU(config)# ip nat inside source list 1 pool h_nat overload

The overload statement indicates that the router will be doing PAT instead of simple NAT; otherwise, problems may arise in relation to the amount of addresses in our pool, since NAT associates one address to one address.

Step 4: Defining the inside and outside interfaces.

This is done in order to specify which interface features the addresses to be translated and which interface deals with the already translated addresses:

Router ANCHORAGE:

ANCHORAGE(config)# interface fastethernet0/0

ANCHORAGE(config-if)# ip nat outside

ANCHORAGE(config)# interface vlan2

ANCHORAGE(config-if)# ip nat inside

Router HONOLULU:

HONOLULU(config)# interface fastethernet0/0

```
HONOLULU(config-if)# ip nat outside
HONOLULU(config)# interface vlan2
HONOLULU(config-if)# ip nat inside
```

With the above configuration it should be possible to ping the TESTING PC (16.16.8.8) from the computers in the networks ANCHORAGE, HONOLULU and the corporate network. It is still necessary to assign a static address to the multipurpose server in the perimeter network in order for the computers, in both HONOLULU and ANCHORAGE, to establish a connection with it. This issue, as well as the general commands for troubleshooting NAT/PAT will be addressed in the following section.

Complete Part B of the Activity review sheet.

PART IV

CONFIGURING STATIC NAT IN THE FIREWALL

In order for the Multipurpose server in the perimeter network to be accessible from the external and the branches networks, it is necessary to set up static NAT configuration; with static configuration the global IP address assigned to a local host will never change, in a dynamic configuration, the global address could be assigned to another host in the internal network if there are many addresses available in the pool. In order to set up static NAT in the HOLLYWOOD02 firewall, the following command is used:

```
HOLLYWOOD02(config)# static (inside, outside) 16.16.8.4 172.16.0.2
```

With the application of the previous command, the server should have access to the external network and vice versa.

Complete Part C of the Activity review sheet.

LABORATORY PRACTICE #2

ACTIVITY REVIEW SHEET

The following are different tasks to be completed by the end of each section of the laboratory guide. Ask the instructor if there is any problem completing any activity.

PART A

1. Access a host in the Anchorage network, a host in the Honolulu network and a host in the Portland network. Enter the command line and try to ping the address 16.16.8.8. Was the ping successful?

   ANCHORAGE: _____ HONOLULU: _____ PORTLAND: _____

2. From the external host specified as 16.16.8.8. Open a web browser and try to access the following addres: http://16.16.8.4 Were you able to access the website? _____

3. From the external host try to ping the address 16.16.8.4. Was the ping successful? _____

Complete Part II of the Laboratory Guide.

PART B

1. Repeat step 1 from part A. Use the *–t* keyword at the end. Was the ping successful this time?

   ANCHORAGE: _____ HONOLULU: _____ PORTLAND: _____

2. From the HONOLULU and ANCHORAGE routers Use the command *show ip nat translations.* From the HOLLYWOOD01 Firewall use the command *show xlate.* A list of the translations that are taking place in the router will be presented. Fill the table:

DEVICE	Inside Global	Inside Local	Outside Global	Outside Local
ANCHORAGE				
ANCHORAGE				
HONOLULU				
HONOLULU				
HOLLYWOOD01				
HOLLYWOOD01				

3. What is the difference between the router command *show ip nat translations* and the firewall command *show xlate*?

4. Briefly define the terms Inside Global, Inside Local, Outside Global and Outside Local.

5. From the external host specified as 16.16.8.8. Open a web browser and try to access the following addres: http://16.16.8.4 Were you able to access the website? _____

6. From the external host try to ping the address 16.16.8.4. Was the ping successful? _____

Complete Part II of the Laboratory Guide.

PART C

1. Repeat steps 5 and 6 from the previous section. Were you able to access the website and ping the IP address? _____ Why? _____

2. From the HOLLYWOOD01 Firewall use the command *show xlate.* Compare your results with the results previously obtained in Part B. What are the differences?

LABORATORY PRACTICE #3

VIRTUAL PRIVATE NETWORKS (VPN)

Objectives

By completing this laboratory practice the student will be able to:

1. Configure the basic parameters for the establishment of a security association (SA) between different sites for VPN purposes by means of Internet Protocol Security (IPsec).
2. Configure Internet Security Association by using Internet Key Exchange (IKE) and Key Management Protocol (ISAKMP) policies for encryption and authentication.
3. Configure data connection parameters for VPN, including transform sets and crypto-maps.

Introduction

Cerveau Inc., needs to connect two branches in Honolulu and Anchorage to the Main Corporate Network through the branch in Los Angeles. The branch in Los Angeles holds the DMZ of the company as well as other services that are only available for the hosts in the internal network. Hosts in Anchorage and Honolulu are able to access the servers in the DMZ but cannot access the hosts or services in the internal network. In order to allow the hosts in these branches to reach the services in the internal network it is necessary to establish a site-to-site VPN connection among the three branches as illustrated in Figure 1.

The routers at the branches of Anchorage and Honolulu will establish a VPN link with the perimeter firewall of Los Angeles (Hollywood02) by using the IPSec protocol suite to define authentication, and encryption mechanisms in order to guarantee confidentiality, integrity and availability of the information that travels between the different branches of the company. By the end of the practice, hosts in Anchorage and Honolulu will have access to FTP and DNS services.

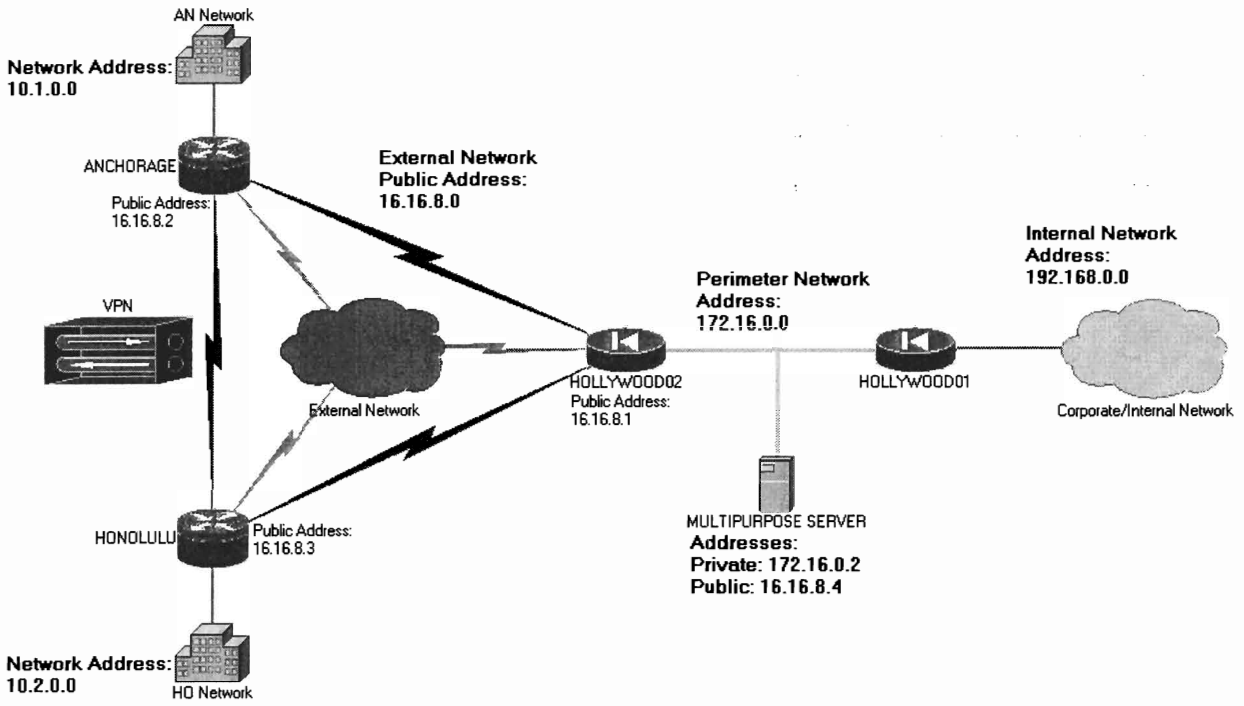


Figure 1. VPN Link Between Anchorage, Honolulu and Hollywood02.

PART I

BASIC CONCEPTS OF VPN AND IPSEC

A VPN is a secure connection between networks that travels over an insecure network infrastructure, usually a public network. In order to build a VPN it is necessary to use a security standard that will vary in accordance to the network characteristics. The security standards consist of different network protocols that are used together to provide authentication, encryption, encapsulation, and integrity assurance of the data.

Among all the security standards used for VPN, one of the most widely present is IPSec, a protocol suite that covers different protocols intended to provide security features to the Internet Protocol (IP). One of the protocols under IPSec is IKE, which is used together with ISAKMP to set up and maintain a VPN connection by generating the authentication keys and the encryption mechanism. IKE goes through two phases in order to establish a successful VPN

connection: Phase 1 builds a secure IPSec management connection, while Phase 2 defines the security protocols that will be used to establish the user connection. Authentication Header (AH) and Encapsulation Security Payload (ESP) are protocols defined during the IKE phase 2 and provide confidentiality, authentication and data integrity. The interaction between all these protocols will be shown in the following sections.

Complete Part A of the Activity review sheet.

PART II

DEFINING THE MANAGEMENT CONNECTION PARAMETERS

In order for two or more networks to support secure communication, a SA needs to be established among these networks; IKE and ISAKMP work together to define two levels of SA, which are the previously mentioned phases. The management connection is established during Phase 1, which defines the session keys used for authentication. This authentication can be based on pre-shared keys, or certificates and digital signatures. It is also in Phase 1, when policies regarding encryption and hashing functions are defined. The following steps need to be followed in order to establish the management connection:

Step 1: Activating and defining the IKE/ISAKMP policies.

These policies will be used for the management connection and include the type of authentication; the encryption algorithm to be used for the management connection; the hashing function for data integrity, which can be either MD5 or SHA; the Diffie-Hellman key group, which sets up a temporary secure connection between the peers; and the lifetime of the management connection. This is done as follow:

Router ANCHORAGE:

```
ANCHORAGE(config)#crypto isakmp enable
```

ANCHORAGE(config)#crypto isakmp policy 1

ANCHORAGE(config-isakmp)#authentication pre-share

ANCHORAGE(config-isakmp)#encryption 3des

ANCHORAGE(config-isakmp)#hash sha

ANCHORAGE(config-isakmp)#group 2

ANCHORAGE(config-isakmp)#lifetime 60000

Router HONOLULU:

HONOLULU(config)#crypto isakmp enable

HONOLULU(config)#crypto isakmp policy 2

HONOLULU(config-isakmp)#authentication pre-share

HONOLULU(config-isakmp)#encryption 3des

HONOLULU(config-isakmp)#hash sha

HONOLULU(config-isakmp)#group 2

HONOLULU(config-isakmp)#lifetime 60000

Firewall HOLLYWOOD02:

HOLLYWOOD02(config)#isakmp enable outside

HOLLYWOOD02(config)#isakmp policy 3 authentication pre-share

HOLLYWOOD02(config)#isakmp policy 3 encrypt 3des

HOLLYWOOD02(config)#isakmp policy 3 hash sha

HOLLYWOOD02(config)#isakmp policy 3 group 2

HOLLYWOOD02(config)#isakmp policy 3 lifetime 60000

Notice the differences and similarities of the commands in the routers and firewall. The first line is used to enable ISAKMP in the devices. In the three cases a number defined by the

network administrator is used as a tag to identify each policy, this number could be the same in the three devices since each of them is independent. The *authentication* parameter indicates the type of authentication that will be used in all cases: a pre-shared key, or password, that will be defined later. The *encryption* indicates the encryption algorithm to be used, in this case it will be triple DES. Finally, the *hash*, *group* and *lifetime* parameters indicate the method for data integrity, the Diffie-Hellman key exchange group and the lifetime of the connection respectively.

Step 2: Defining the pre-shared key.

This key refers to the password that will be used by each of the peers to establish the secure connection. In this case, for each router or firewall, we have to define the shared secret for the peers that will be establishing a connection as follow:

Router ANCHORAGE:

ANCHORAGE(config)#crypto isakmp key vpnkey4411 address 16.16.8.1

ANCHORAGE(config)#crypto isakmp key vpnkey4411 address 16.16.8.3

Router HONOLULU:

HONOLULU(config)#crypto isakmp key vpnkey4411 address 16.16.8.1

HONOLULU(config)#crypto isakmp key vpnkey4411 address 16.16.8.2

Firewall HOLLYWOOD02:

HOLLYWOOD02(config)# isakmp key vpnkey4411 address 16.16.8.2

HOLLYWOOD02(config)# isakmp key vpnkey4411 address 16.16.8.3

Since there are three devices participating in the VPN, each device must have the pre-shared keys of the other two. The *address* parameter indicates the address of the neighbor that the device will try to contact by using the pre-shared key.

Complete Part B of the Activity review sheet.

PART III

DEFINING THE DATA LINK PARAMETERS

The data link or VPN tunnel is established during the IKE phase 2, this second SA is established by means of the transform sets, which manage the encryption and message integrity methods to be used for the IPSec Tunnel. These transform sets define which protocols will be used for authentication and the encryption mechanism, with different combinations of AH and ESP. The transform sets need to be associated with a crypto map for each VPN connection that is being established. After the traffic that will go through the VPN has been defined and the crypto map activated, the SA is established and the VPN link is usable. This section covers the concepts of transform set and crypto map as well as the necessary steps to establish the data link.

Step 1: Configuring a transform set.

The transform set can accept up to three different combinations of AH and ESP protocols with an encryption and hash algorithm pair; each of this combination is known as a transform. The transform set has a unique case sensitive name that will be provided by the network administrator, followed by the transforms that will be used, ordered by priority:

Router ANCHORAGE:

ANCHORAGE(config)#crypto ipsec transform-set vpnAnchor esp-3des esp-sha-hmac

ANCHORAGE(cfg-crypto-trans)#exit

Router HONOLULU:

HONOLULU(config)#crypto ipsec transform-set vpnHono esp-3des esp-sha-hmac

HONOLULU(cfg-crypto-trans)#exit

Firewall HOLLYWOOD02:

HOLLYWOOD02(config)#crypto ipsec transform-set vpnHolly esp-3des esp-sha-hmac

In the instruction name defined by the network administrator follows the *transform-set* statement. The transforms to be used are defined right after the name; in this case we are using two transforms out of the three available per transform set. A remote client could use any available transform to establish a SA, but the first one, which in this case is ESP protocol with 3DES encryption, is the one that takes priority. Notice that the name of each transform set doesn't necessarily match with the name given by each device.

Step 2: Configuring a crypto access-list.

The crypto access-list is used to define the traffic that will go through the VPN tunnel. This is access list indicates the traffic that will be sent through the VPN tunnel. Each device will establish a connection for the three networks that will be participating in the VPN as follow:

Router ANCHORAGE:

ANCHORAGE(config)#access-list 101 permit ip 10.1.0.0 0.0.255.255 10.2.0.0 0.0.255.255

ANCHORAGE(config)#access-list 102 permit ip 10.1.0.0 0.0.255.255 172.16.0.0 0.0.255.255

ANCHORAGE(config)#access-list 103 permit ip 10.1.0.0 0.0.255.255 192.168.0.0 0.0.255.255

Router HONOLULU:

HONOLULU(config)#access-list 101 permit ip 10.2.0.0 0.0.255.255 10.1.0.0 0.0.255.255

HONOLULU(config)#access-list 102 permit ip 10.2.0.0 0.0.255.255 172.16.0.0 0.0.255.255

HONOLULU(config)#access-list 103 permit ip 10.2.0.0 0.0.255.255 192.168.0.0 0.0.255.255

Firewall HOLLYWOOD02:

HOLLYWOOD02(config)#access-list to_anchor1 permit ip 192.168.0.0 255.255.0.0 10.1.0.0 255.255.0.0

HOLLYWOOD02(config)#access-list to_anchor2 permit ip 172.16.0.0 255.255.0.0 10.1.0.0 255.255.0.0

HOLLYWOOD02(config)#access-list to_hono1 permit ip 192.168.0.0 255.255.0.0 10.2.0.0 255.255.0.0

HOLLYWOOD02(config)#access-list to_hono2 permit ip 172.16.0.0 255.255.0.0 10.2.0.0 255.255.0.0

Since the firewall deals with both the DMZ and the internal network, it is necessary to define both networks in the ACLs, otherwise the traffic from the DMZ will not be reachable through the VPN tunnel, and this is done for cases in which services inside the DMZ are not reachable from the outside networks.

Step 3: Configuring a crypto map to each participating destination.

The crypto maps reunites all the information that is required to establish the SA, including the identity of the peers, the way that the SA will be established by means of ISAKMP/IKE, the traffic that will go through the VPN and how this will be established; these last two functions are done by associating the transform set and the ACLs defined previously. A crypto map, just like in the case of a transform set will have a name provided by the network administrator; following this name is a sequence number which will define priority in the case of

Router ANCHORAGE:

ANCHORAGE(config)#crypto map vpn_tunnel 1 ipsec-isakmp

ANCHORAGE(config-crypto-map)#match address 101

ANCHORAGE(config-crypto-map)#set peer 16.16.8.3

ANCHORAGE(config-crypto-map)#set transform-set vpnAnchor

ANCHORAGE(config-crypto-map)#exit

With the previous commands a VPN tunnel to HONOLULU has been configured, notice that the *match address* command refers to an access list defined in the previous step. The

command *set peer* refers to the public address of the router that will be participating in the VPN. Finally, the command *set transform-set* associates the transform previously defined with the crypto map. Now it is time to define the parameters for the two connections that will be going to HOLLYWOOD, this is done in a similar way to the case that has just been presented. Notice that the starting command indicates both a name for the crypto map, in this case *vpn_tunnel*, plus a number tag that differentiates each section:

```
ANCHORAGE(config)#crypto map vpn_tunnel 2 ipsec-isakmp
ANCHORAGE(config-crypto-map)#match address 102
ANCHORAGE(config-crypto-map)#set peer 16.16.8.1
ANCHORAGE(config-crypto-map)#set transform-set vpnAnchor
ANCHORAGE(config-crypto-map)#exit
ANCHORAGE(config)#crypto map vpn_tunnel 3 ipsec-isakmp
ANCHORAGE(config-crypto-map)#match address 103
ANCHORAGE(config-crypto-map)#set peer 16.16.8.1
ANCHORAGE(config-crypto-map)#set transform-set vpnAnchor
ANCHORAGE(config-crypto-map)#exit
```

The same procedure must be applied to HONOLULU in order to establish the VPN connections to its neighbors:

Router HONOLULU:

```
HONOLULU(config)#crypto map vpn_tunnel 1 ipsec-isakmp
HONOLULU(config-crypto-map)#match address 101
HONOLULU(config-crypto-map)#set peer 16.16.8.2
HONOLULU(config-crypto-map)#set transform-set vpnHono
```

HONOLULU(config-crypto-map)#exit

HONOLULU(config)#crypto map vpn_tunnel 2 ipsec-isakmp

HONOLULU(config-crypto-map)#match address 102

HONOLULU(config-crypto-map)#set peer 16.16.8.1

HONOLULU(config-crypto-map)#set transform-set vpnHono

HONOLULU(config-crypto-map)#exit

HONOLULU(config)#crypto map vpn_tunnel 3 ipsec-isakmp

HONOLULU(config-crypto-map)#match address 103

HONOLULU(config-crypto-map)#set peer 16.16.8.1

HONOLULU(config-crypto-map)#set transform-set vpnHono

HONOLULU(config-crypto-map)#exit

A VPN in a firewall follows the same principle with slight changes. This can be seen in the following configuration:

Firewall HOLLYWOOD02:

HOLLYWOOD02(config)#crypto map vpn_tunnel 1 ipsec-isakmp

HOLLYWOOD02(config)#crypto map vpn_tunnel 1 match address to_anchor1

HOLLYWOOD02(config)#crypto map vpn_tunnel 1 set peer 16.16.8.2

HOLLYWOOD02(config)#crypto map vpn_tunnel 1 set transform-set vpnHolly

HOLLYWOOD02(config)#crypto map vpn_tunnel 2 ipsec-isakmp

HOLLYWOOD02(config)#crypto map vpn_tunnel 2 match address to_anchor2

HOLLYWOOD02(config)#crypto map vpn_tunnel 2 set peer 16.16.8.2

HOLLYWOOD02(config)#crypto map vpn_tunnel 2 set transform-set vpnHolly

The previous block presents the configuration of the VPN links that connect the two networks in California (DMZ and Internal) to the Anchorage network. The same must be done to establish the link to Honolulu, the defining factors about the link are the peer and the match address ACL that is being used.

HOLLYWOOD02(config)#crypto map vpn_tunnel 3 ipsec-isakmp

HOLLYWOOD02(config)#crypto map vpn_tunnel 3 match address to_hono1

HOLLYWOOD02(config)#crypto map vpn_tunnel 3 set peer 16.16.8.3

HOLLYWOOD02(config)#crypto map vpn_tunnel 3 set transform-set vpnHolly

HOLLYWOOD02(config)#crypto map vpn_tunnel 4 ipsec-isakmp

HOLLYWOOD02(config)#crypto map vpn_tunnel 4 match address to_hono2

HOLLYWOOD02(config)#crypto map vpn_tunnel 4 set peer 16.16.8.3

HOLLYWOOD02(config)#crypto map vpn_tunnel 4 set transform-set vpnHolly

Step 4: Associating a crypto map with an external interface.

In order to establish a working VPN connection, the crypto map needs to be associated with an external interface in a similar way to access lists. This is done as follows:

Router ANCHORAGE:

ANCHORAGE(config)#interface fastethernet 0/0

ANCHORAGE(config-if)#crypto map vpn_tunnel

Router HONOLULU:

HONOLULU(config)#interface fastethernet 0/0

HONOLULU(config-if)#crypto map vpn_tunnel

Firewall HOLLYWOOD02:

HOLLYWOOD02(config)#crypto map vpn_tunnel interface outside

Step 5: Defining the address that will not participate in the NAT process.

This is done by creating a new access list to be used in the NAT process:

Router ANCHORAGE:

ANCHORAGE(config)#access-list 199 deny ip 10.1.0.0 0.0.255.255 10.2.0.0 0.0.255.255

ANCHORAGE(config)#access-list 199 deny ip 10.1.0.0 0.0.255.255 172.16.0.0 0.0.255.255

ANCHORAGE(config)#access-list 199 deny ip 10.1.0.0 0.0.255.255 192.168.0.0 0.0.255.255

ANCHORAGE(config)#access-list 199 permit ip 10.1.0.0 0.0.255.255 any

Router HONOLULU:

HONOLULU(config)#access-list 199 deny ip 10.2.0.0 0.0.255.255 10.1.0.0 0.0.255.255

HONOLULU(config)#access-list 199 deny ip 10.2.0.0 0.0.255.255 172.16.0.0 0.0.255.255

HONOLULU(config)#access-list 199 deny ip 10.2.0.0 0.0.255.255 192.168.0.0 0.0.255.255

HONOLULU(config)#access-list 199 permit ip 10.2.0.0 0.0.255.255 any

Firewall HOLLYWOOD02:

HOLLYWOOD02(config)#access-list no_nat permit ip 172.16.0.0 255.255.0.0 10.0.0.0 255.0.0.0

HOLLYWOOD02(config)#access-list no_nat permit ip 192.168.0.0 255.255.0.0 10.0.0.0 255.0.0.0

Step 6: Associating the access list to the NAT process.

The firewall can associate the access list by the adition of a single instruction. In the case of the routers, due to the complexity of the access list, the creation of a route map that comprises the access list policies is needed. The route map will be associated with the inside source list and then it will substitute the NAT source list that was created in the previous laboratory practice. This will be done as follows:

Router ANCHORAGE:

ANCHORAGE(config)#route-map vpn_nat permit 10

ANCHORAGE(config-route-map)#match ip address 199

ANCHORAGE(config-route-map)#exit

ANCHORAGE(config)#ip nat inside source route-map vpn_nat pool a_nat overload

ANCHORAGE(config)#no ip nat inside source list 1 pool a_nat overload

Router HONOLULU:

HONOLULU(config)#route-map vpn_nat permit 10

HONOLULU(config-route-map)#match ip address 199

HONOLULU(config-route-map)#exit

HONOLULU(config)#ip nat inside source route-map vpn_nat pool h_nat overload

HONOLULU(config)#no ip nat inside source list 1 pool h_nat overload

Firewall HOLLYWOOD02:

HOLLYWOOD02(config)#nat (inside) 0 access-list no_nat

Step 7: Allowing IPSec traffic into the Firewall.

This is done by adding the following command in the firewall:

Firewall HOLLYWOOD02:

HOLLYWOOD02(config)#sysopt connection permit-ipsec

This makes any traffic that belongs to the VPN connections participate in the internal network as if they belonged to it; otherwise the traffic will be restricted as outside traffic.

Complete Part C of the Activity review sheet.

LABORATORY PRACTICE #3

ACTIVITY REVIEW SHEET

The following are different tasks to be completed by the end of each section of the laboratory guide. Ask the instructor if there is any problem completing any activity.

PART A

1. Pick one host from the remote branches (Either Anchorage or Honolulu) and one in the Internal Network. Record the following information by means of the *ipconfig /all* command:

   Host 01:

   Network Name: _____

   IP address and Mask: _____

   Default Gateway/Router: _____

   DNS Server: _____

   Host 02:

   Network Name: _____

   IP address and Mask: _____

   Default Gateway/Router: _____

   DNS Server: _____

2. Verify that the remote branches can reach the External Network. From Host 01 try to ping the public addresses of your neighbors as presented below (You won't reach your own public address) Record the results:

   16.16.8.1: _____

   16.16.8.2: _____

   16.16.8.3: _____

3. Verify that services such as FTP and DNS are not available for the external networks. Open a web browser and enter the following URL: http://www.cerveau.com Was the website displayed? _____

   From the web browser enter the following address: ftp://172.16.0.2 Were you able to access the FTP server? _____

Complete Part II of the Laboratory Guide.

PART B

From your console, verify the configuration using the following commands from the privileged exec mode:

1. *show crypto isakmp key*

This command will provide with information regarding the password that will be used by the remote sites to establish a phase 1 security association for management. Record the Hosts and the key/password used to establish the security association.

_____

_____

2. *show crypto isakmp policy*

This command will provide you with information regarding the parameters that will be used for establishing the phase 1 security association. Record the parameters for the Protection suite of priority. Do they match with the parameters defined in Step 1. Part II of the guide?

_____

_____

_____

_____

3. *show crypto ipsec sa*

Information regarding this command will be provided later. Does this command show any information related to the security associations? _____

Complete Part III of the Laboratory Guide.

PART C

1. Verify that there is connectivity between the remote networks and the internal network. Pick one computer in the internal network and try to ping the following addresses: 10.1.0.2, 10.2.0.2. Was the ping successful? _____
2. From your console, verify the state of the connections by using the following commands from the privileged exec mode:

   show crypto ipsec sa

   This command will provide information regarding to the phase 2 security association. Search for the association between your public address and any other peer. Record the information related to the packets in that association.

   Peers IP addresses: _____

   Packets encrypted: _____

   Packets decrypted: _____

   show crypto isakmp sa

   This command presents information about the management connections of the phase 1 security association. Record the addresses of the participant peers and the status of the association. Were the sessions established or are they still pending?

_____

_____

3. Study the behavior of the VPN tunnel. From one of the remote routers console try to ping the Server 172.16.0.2. Was the ping successful? _____ Try again by issuing the following command: *ping 172.16.0.2 source vlan 2*. Was the ping successful? _____ Why?

   _____

   _____

4. Verify the availability of services for the hosts of the remote networks. Open a web browser in Host 1 and enter the following URL: http://www.cerveau.com Was the website displayed?

   _____

   Try to access the ftp server from the website. Were you able to do it? _____

   Notice that members of the remote networks are no longer restricted as part of the External Network.

LABORATORY PRACTICE #4

IMPLEMENTATION OF VOICE OVER IP (VoIP)

Objectives

By completing this laboratory practice the student will be able to:

1. Configure virtual local area networks (VLANs) for data traffic and voice.
2. Configure quality of service (QoS) parameters to be used in Voice over IP (VoIP).
3. Configure dynamic host configuration protocol (DHCP) services in the router.
4. Configure ports in a switch for VoIP.
5. Configure IP phones features.
6. Verify communication between VoIP devices.

Introduction

Cerveau, Inc., a company with branches in both Anchorage (AK) and Honolulu (HI) has decided to reduce the amount of their telephone bills by creating a VoIP infrastructure that will reduce the cost of long distance calls between the two branches by means of VoIP packets traveling over the WAN link. As a network administrator, you have been asked to establish the basis of the VoIP infrastructure in both sites, as well as the connection between the long distance peers. Details of the desired architecture can be seen in Figure 1.

The Cisco 2800 series routers have both integrated switch capability and the Cisco Unified Communication Manager Express Suite. The IP Phone models to be used are the Cisco 7961 and 7941 series. This practice involves the creation of phone directory parameters, the association between IP phones and the directory numbers, and the configuration of a communication link between remote sites by modifying an existing infrastructure. Before starting, carefully review the subnetting structure presented in Figure 1.

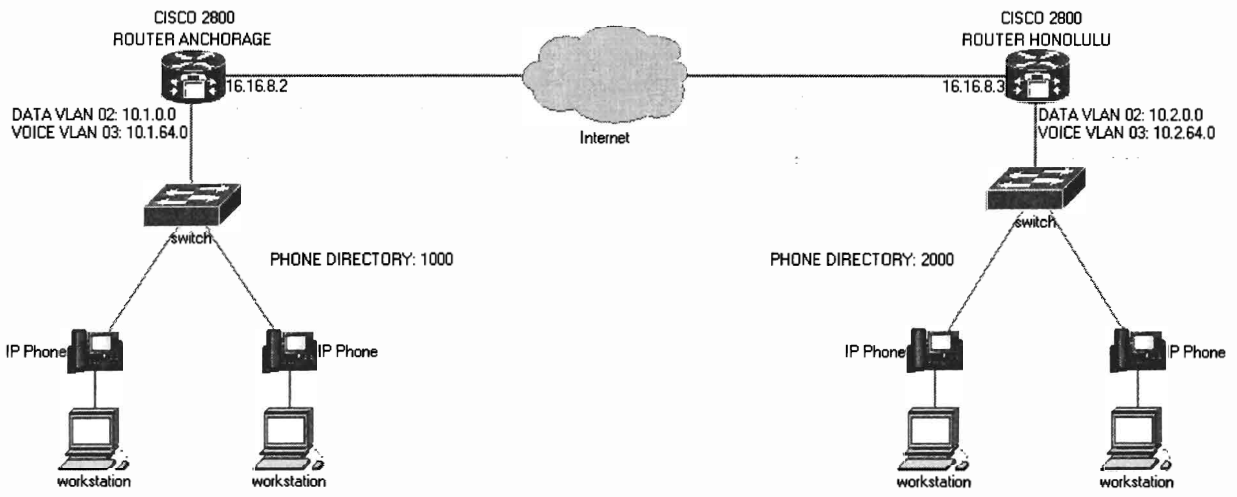


Figure 1. Desired VoIP infrastructure for the two branches.

PART I

BASIC CONCEPTS OF TELEPHONE NETWORKS

Telephone networks originally consisted on analog phones that converted voice signals into electrical signals which were transmitted over the Public Switched Telephone Network (PSTN), as the name implies, PSTN consisted of a public telephone network hierarchically arranged by Telephone Exchanges, also known as telephone switches. If a company wanted to have a private phone network they needed to build it separated from the data network with the help of a Private Branch Exchange (PBX), which resulted in a significant investment. Nowadays, VoIP allows the delivery of voice communications over the computer network infrastructure; this not only reduces cost in terms of building infrastructure, but allows for more versatility and can also reduce costs in terms of long distance calls, as exemplified in the introduction.

There are many factors to be considered in order to properly implement a VoIP infrastructure, some of these factors are similar to the PBX telephone networks while other factors are totally unrelated. Among these factors, QoS plays in an important role in order to

ensure that the voice transmission is clear to both the receiver and receptor. Although QoS is not a new issue in telephone networks, the approach that it takes when switching to a data network presents significant differences: it is important to consider that in data networks, packets might take different routes to a common destination, arriving at different intervals and order, and the available channel capacity might become a problem when delivering multimedia traffic that takes a higher priority; it is for these problems that QoS needs to be addressed in VoIP networks.

VoIP networks cover a wide range of technologies, some of them are optional like Power over Ethernet (PoE); other technologies, like VLANs are necessary for the coexistence of both data and voice traffic over the same link and for the proper security of voice traffic.

Complete Part A of the Activity review sheet.

PART II

CONFIGURING VLANs AND QoS

A VLAN, is a logical LAN or broadcast domain created with the help of a switch or switches. A switch that doesn't support VLANs works as a single broadcast domain, if another switch is connected then the broadcast domain is extended. In order to separate or divide a broadcast domain a router becomes necessary. Switches with VLAN capabilities can host different broadcast domain in the form of VLANs, the VLAN configuration of a switch can be replicated manually to other switches; or automatically by means of VLAN Trunking Protocol (VTP); in this way, devices that are physically separated can contact each other as long as they are part of the same VLAN, as part of the same broadcast domain.

The convenience of VLANs for VoIP comes from the standard IEEE 802.1Q, also known as VLAN tagging, which allows the sharing of a single physical Ethernet network link by multiple VLANs. Voice traffic can travel together with data traffic under the same link when

multiple VLANs are implemented. This not only ensures convergence of voice and data, but also secures voice traffic. Before connecting the phones to the data network it is important to properly define a VLAN to be used by voice traffic and separate it from the data traffic. This is done as follow:

Step 1: Deactivating VTP by setting the mode to transparent.

As previously defined, VTP permits the automatic redistribution of VLAN configuration. In many cases this protocol is deactivated, particularly in the case of high security network, because of the danger of a rogue switch sending inaccurate or altered VLAN information.

Router ANCHORAGE:

ANCHORAGE(config)#vtp mode transparent

Router HONOLULU:

HONOLULU(config)#vtp mode transparent

Step 2: Identifying a VLAN for data traffic.

The computers inside this VLAN will need a gateway which will be defined by accessing the configuration mode of the VLAN interface. VLAN 2 has been used so far for data traffic. In this case, the parameters will provide a description of the interface functions:

Router ANCHORAGE:

ANCHORAGE(config)#vlan 2

ANCHORAGE(config-vlan)#name DATA

ANCHORAGE(config-vlan)#interface vlan 2

ANCHORAGE(config-if)#description Data_Services

Router HONOLULU:

HONOLULU(config)#vlan 2

HONOLULU(config-vlan)#name DATA

HONOLULU(config-vlan)#interface vlan 2

HONOLULU(config-if)#description Data_Services

The number identifiers, name of the VLAN, description of the interface and ip addresses (which was defined previously) are parameters defined by the network administrator. In this sense, it is possible to use a VLAN 10 or any other valid number, the same goes for names and descriptions, which could have been VoIP or any other alternative name.

Step 3: Defining and activating a VLAN for voice traffic.

VLAN 3 will be used for voice traffic, and the interface VLAN 3 will define the gateway (or source address) for the IP phones.

Router ANCHORAGE:

ANCHORAGE(config)#vlan 3

ANCHORAGE(config-vlan)#name VOICE

ANCHORAGE(config-vlan)#interface vlan3

ANCHORAGE(config-if)#description Telephone_Services

ANCHORAGE(config-if)#ip address 10.1.64.1 255.255.192.0

ANCHORAGE(config-if)#no shutdown

Router HONOLULU:

HONOLULU(config)#vlan 3

HONOLULU(config-vlan)#name VOICE

HONOLULU(config-vlan)#interface vlan 3

HONOLULU(config-if)#description Telephone_Services

HONOLULU(config-if)#ip address 10.2.64.1 255.255.192.0

```
HONOLULU(config-if)#no shutdown
```

Step 4: Configuring the ports of the switch.

This includes assigning VLANs to the switches and setting the QoS parameters.

Router ANCHORAGE:

```
ANCHORAGE(config)#interface range fastEthernet 0/1/0 – 3
ANCHORAGE(config-if-range)#switchport mode access
ANCHORAGE(config-if-range)#switchport access vlan 2
ANCHORAGE(config-if-range)#switchport voice vlan 3
ANCHORAGE(config-if-range)#auto qos voip trust
```

Router HONOLULU:

```
HONOLULU(config)#interface range fastEthernet 0/1/0 – 3
HONOLULU(config-if-range)#switchport mode access
HONOLULU(config-if-range)#switchport access vlan 2
HONOLULU(config-if-range)#switchport voice vlan 3
HONOLULU(config-if-range)#auto qos voip trust
```

The last instruction defines the QoS characteristics of the channel. Auto QoS uses a queuing method known as low latency queuing (LLQ) which provides a particular bandwidth to different types of traffic based on the QoS marking that it has. The voice traffic will undergo a QoS bandwidth assignment. Since these markings can be modified by the user if they have special software, some switches can actually specify the type of device to be trusted, such as a Cisco IP Phone or Cisco softphone.

The Cisco 2800 series routers in the laboratory possess an integrated switch, which can only establish the auto QoS parameters with the Trust directive. In the case of networks that use

devices of different manufactures the directive *trust* indicates that it will trust all type of QoS markings indicating that the traffic is voice traffic.

Complete Part B of the Activity review sheet.

PART III

CONFIGURING DHCP SERVICES AND ROUTER CLOCK

DHCP is a protocol that allows the dynamic configuration of Ip addresses in hosts as well as other parameters such as DNS and Gateways. DHCP is important in the context of VoIP because IP Phones need both a dial number and an Ip address, the latest is assigned by the DHCP server by following these steps:

Step 1: Defining the addresses that will not participate in the DHCP process.

DHCP works by assigning address to the host that are connected to the network from a pool of available addresses. It is important to exclude from this pool any address that is assigned for something in particular. In this case, the addresses that will be excluded are the gateways for both the data and the voice networks:

Router ANCHORAGE:

ANCHORAGE(config)#ip dhcp excluded-address 10.1.0.1

ANCHORAGE(config)#ip dhcp excluded-address 10.1.64.1

Router HONOLULU:

HONOLULU(config)#ip dhcp excluded-address 10.2.0.1

HONOLULU(config)#ip dhcp excluded-address 10.2.64.1

Step 2: Defining a DHCP pool for data traffic.

The name of the pool will be defined in the first instruction by the network administrator. In this case, the pool for data traffic will be named PC_DEV. Other parameters that are

configured in the pool are the ip address range (subnet) included in the pool, the default gateway and the DNS server.

Router ANCHORAGE:

```
ANCHORAGE(config)#ip dhcp pool PC_DEV
ANCHORAGE(dhcp-config)#network 10.1.0.0 255.255.192.0
ANCHORAGE(dhcp-config)#default-router 10.1.0.1
ANCHORAGE(dhcp-config)#dns-server 172.16.0.2
ANCHORAGE(dhcp-config)#exit
```

Router HONOLULU:

```
HONOLULU(config)#ip dhcp pool PC_DEV
HONOLULU(dhcp-config)#network 10.2.0.0 255.255.192.0
HONOLULU(dhcp-config)#default-router 10.2.0.1
HONOLULU(dhcp-config)#dns-server 172.16.0.2
HONOLULU(dhcp-config)#exit
```

Step 3: Defining a DHCP pool for voice traffic.

In the case of voice traffic, in addition to the basic parameters, it is important to define a tftp server for the IP Phones to download configuration files and firmware updates. A tftp server is assigned with the instruction *option 150 ip*. The option command provides a range of raw DHCP options that are identified by numerical codes. Code 150 indicates that the ip address that follows is a tftp server; in this case, the tftp server is the router.

Router ANCHORAGE:

```
ANCHORAGE(config)#ip dhcp pool PH_DEV
ANCHORAGE(dhcp-config)#network 10.1.64.0 255.255.192.0
```

ANCHORAGE(dhcp-config)#default-router 10.1.64.1

ANCHORAGE(dhcp-config)#option 150 ip 10.1.64.1

ANCHORAGE(dhcp-config)#exit

Router HONOLULU:

HONOLULU(config)#ip dhcp pool PH_DEV

HONOLULU(dhcp-config)#network 10.2.64.0 255.255.192.0

HONOLULU(dhcp-config)#default-router 10.2.64.1

HONOLULU(dhcp-config)#option 150 ip 10.2.64.1

HONOLULU(dhcp-config)#exit

Step 4: Configuring time settings in the router.

The last step before the actual configuration of the VoIP infrastructure is the definition of time settings for the router. The time settings are necessary in order to keep an appropriate record of the last modification of the configuration files that are used by the IP Phones.

Router ANCHORAGE:

ANCHORAGE(config)#clock timezone CST –6

ANCHORAGE(config)#do clock set *hh:mm:ss month dd year*

Router HONOLULU:

HONOLULU(config)#clock timezone CST –6

HONOLULU(config)#do clock set *hh:mm:ss month dd year*

The *timezone* command , as it name implies, sets the time zone in accordance to the location, which in this case is CST -6. In order to actually define the time it is necessary to use the *clock set* command, which can be accessed from the PRIVILEGED EXEC mode, or from the

configuration mode by adding the keyword *do*; it is important to follow the syntax in order to properly define the time. As an example we can do:

ROUTER(config)#do clock set 14:34:12 January 02 2011.

Complete Part C of the Activity review sheet.

PART IV

CONFIGURING VOIP WITH CISCO UNIFIED CME

CME stands for Communication Manager Express. The simplicity of CME and the fact that it can be preinstalled in Cisco Routers allows the student that is entering the VoIP field to easily understand key concepts in the area without the need of a dedicated VoIP server. This section covers a basic configuration of CME in order to allow traffic in a single branch.

Step 1: Defining the maximum number of phones and directory numbers.

In order to define these parameters it is necessary to access the configuration mode of CME by using the command *telephony-service* from the configuration mode.

Router ANCHORAGE:

ANCHORAGE(config)#telephony-service

ANCHORAGE(config-telephony)#max-ephones 4

ANCHORAGE(config-telephony)#max-dn 4

Router HONOLULU:

HONOLULU(config)# telephony-service

HONOLULU(config-telephony)#max-ephones 4

HONOLULU(config-telephony)#max-dn 4

The commands *max-ephones* and *max-dn* define the maximum number of telephones and directory numbers respectively. These numbers will not always the same.

Step 2: Defining the directory numbers.

The directory numbers are basically the number that the users will have to dial in order to reach a phone. For this practice two numbers will be configured for each CME router. The command *ephone-dn* followed by a number identifier defined by the network administrator provides access to the directory number configuration. The number identifier, also known as tag will also be useful to associate this number with a phone.

Router ANCHORAGE:

ANCHORAGE(config)#ephone-dn 1

ANCHORAGE(config-ephone-dn)#number 1001

ANCHORAGE(config-ephone-dn)#exit

ANCHORAGE(config)#ephone-dn 2

ANCHORAGE(config-ephone-dn)#number 1011

ANCHORAGE(config-ephone-dn)#exit

Router HONOLULU:

HONOLULU(config)#ephone-dn 1

HONOLULU(config-ephone-dn)#number 2001

HONOLULU(config-ephone-dn)#exit

HONOLULU(config)#ephone-dn 2

HONOLULU(config-ephone-dn)#number 2011

HONOLULU(config-ephone-dn)#exit

Step 3: Associating IP Phones with the directory numbers.

This is done by entering the command *ephone* followed by a tag that will identify the IP Phone. After this, the administrator is free to enter the desired configuration of the phone.

Router ANCHORAGE:

ANCHORAGE(config)#ephone 1

ANCHORAGE(config-ephone)#mac-address *xxxx.xxxx.xxxx*

ANCHORAGE(config-ephone)#button 1:1

ANCHORAGE(config-ephone)#exit

ANCHORAGE(config)#ephone 2

ANCHORAGE(config-ephone)#mac-address *yyyy.yyyy.yyyy*

ANCHORAGE(config-ephone)#button 1:2

ANCHORAGE(config-ephone)#exit

Router HONOLULU:

HONOLULU(config)#ephone 1

HONOLULU(config-ephone)#mac-address *xxxx.xxxx.xxxx*

HONOLULU(config-ephone)#button 1:1

HONOLULU(config-ephone)#exit

HONOLULU(config)#ephone 2

HONOLULU(config-ephone)#mac-address *yyyy.yyyy.yyyy*

HONOLULU(config-ephone)#button 1:2

HONOLULU(config-ephone)#exit

The configuration paramenters presented in this case are MAC addresses and directory number assignation. The association between the directory numbers and the telephone is done with the *button* command; this actually refers to the buttons located to the right of the display panel in the IP Phones; the directory number is the one after the colon sign, which gives the following sintax: button *ip_phone_button : directory_number*

Step 4: Creating the configuration file for the IP Phones.

To create a valid configuration file, it is important to specify the address that the phones need to contact in order to reach the CME router.

Router ANCHORAGE:

ANCHORAGE(config)#telephony-service

ANCHORAGE(config-telephony)#ip source-address 10.1.64.1

ANCHORAGE(config-telephony)#no create cnf-files

ANCHORAGE(config-telephony)#create cnf-files

Router HONOLULU:

HONOLULU(config)#telephony-service

HONOLULU(config-telephony)#ip source-address 10.2.64.1

HONOLULU(config-telephony)#no create cnf-files

HONOLULU(config-telephony)#create cnf-files

The command *create cnf-file* will either create or update an existing configuration file that will be used by the phones that will be connected to the switch. The no create cnf-file is used to delete any previous configuration file that might exist. It is important to indicate that the *ip source address*, which is the CME router address doesn't necessarily has to be the gateway defined in the VLAN interface. Depending on the circumstances, the creation of a loopback address within the CME router might be necessary in order to refer the IP Phones to it.

Step 5: Connecting the IP phones to the integrated switch and troubleshooting.

After all the settings have been successfully introduced in the routers, the IP phones can be connected to the integrated switch of the router. IP phones have two ports on their backside, it

is important to make sure that the port that reads *switch* is connected to the integrated switch.

Complete Part D of the Activity review sheet.

PART V

CONFIGURING VOIP BETWEEN REMOTE SITES

To establish a connection to a remote site it is necessary to configure a dial peer. A dial peer works like a static route, defining the path that voice traffic will take to reach a different voice network. This network can be a VoIP network or a traditional voice network. This is specified with the command *dial-peer*, which uses a number identifier defined by the administrator, followed by the type of voice network that has to be configured.

Router ANCHORAGE:

ANCHORAGE(config)#dial-peer voice 1 voip

ANCHORAGE(config-dial-peer)#destination-pattern 2...

ANCHORAGE(config-dial-peer)#session target ipv4:16.16.8.3

Router HONOLULU:

HONOLULU(config)#dial-peer voice 1 voip

HONOLULU(config-dial-peer)#destination-pattern 1...

HONOLULU(config-dial-peer)#session target ipv4:16.16.8.2

The dots in the *destination-pattern* command work as a wildcard that indicates the way that the directory numbers are organized in the other side of the connection. The *session target* command defines the next hop that the voice traffic will take to reach the voice network.

Complete Part E of the Activity review sheet.

LABORATORY PRACTICE #4

ACTIVITY REVIEW SHEET

The following are different tasks to be completed by the end of each section of the laboratory guide. Ask the instructor if there is any problem completing any activity.

PART A

1. Verify that the host associated with your router is connected to the integrated switch in the router. Access the host and record the IP configuration by using ipconfig /all:

   IP address/Mask: _____

   Default Gateway/Router: _____

   Is DHCP enabled? _____

2. Connect the IP phones to the cisco 2800 routers integrated switch. One in each router. Wait until the phones are displaying the date. Press the button marked with a check symbol over two squares and access the Network Configuration. Record the following information if possible, write N/A if not available:

   Phone 1:

   MAC Address: _____

   IP address/Mask: _____

   Default Gateway/Router: _____

   TFTP Server: _____

   Phone 2:

   MAC Address: _____

   IP address/Mask: _____

   Default Gateway/Router: _____

TFTP Server: _____

3. Disconnect the IP phones.

Complete Part II of the Laboratory Guide.

PART B

1. Using the command *show vtp status* from the privileged exec mode, record the following information:

   VPT Version: _____

   Number of existing VLANs: _____

   VTP Operating Mode: _____

2. Using the command *show running-config* verify the VLAN configuration of the router.

   VLAN for voice: _____

   VLAN for data: _____

   Complete Part III of the Laboratory Guide.

PART C

1. Enter the command *show clock* on your router from the privileged exec mode. Record the time as shown in the console. _____

2. Access the host associated with your router and change the ip setting to DHCP enabled. Go to your console and enter the command *ip config /all*

   Was the address assignment successful? ____ If no, check the router configuration.

   Record the time when the lease expires: _____

   Complete Part IV of the Laboratory Guide.

PART D

1. Using the command *show telephony-service tftp-binding* list some of the configuration files available for the phones to download:

   _____

2. After connecting the IP phones to the router, did the screen menu on the phones changed in any way after the connection? ____ Record the changes.

   _____

3. Use the *show ephone* command in your router:

   Are both phones registered? _____ If they aren't. Contact the instructor.

4. Access the Network Configuration on the phone. Record the following information if possible, write N/A if not available:

   Phone 1:

   MAC Address: _____

   IP address/Mask: _____

   Default Gateway/Router: _____

   TFTP Server: _____

   Phone 2:

   MAC Address: _____

   IP address/Mask: _____

   Default Gateway/Router: _____

   TFTP Server: _____

   Does the IP address associated with the MAC address of the phone match the records in the router?_____

5. From the priviledged exec mode enter the command *debug ephone register*. Enter the configuration mode and use the following commands:

   ANY_ROUTER(config)#telephony-service

   ANY_ROUTER(config-telephony)#reset *xxxx.xxxx.xxxx*

Where the x might represent the format of a MAC address. What happened?

_____

_____

_____

Complete Part V of the Laboratory Guide.

PART E

1. Disconnect one of the phones from one router and connect it in the other, wait for it to register. Did the phone display change in any way? ____ Record the changes:

   _____

2. From the router enter the command *show telephony-service dial-peer* in the privileged exec mode. Record the remote peers information. _____

LABORATORY PRACTICE #5

802.11 WIRELESS LOCAL AREA NETWORKS

Objectives

By completing this laboratory practice the student will be able to:

1. Configure the basic settings of an infrastructure Wireless Local Area Network (WLAN)
2. Define the Service Set Identifiers of a WLAN and their behavior.
3. Perform the basic configuration of radio channels and define the behavior of the antennas.
4. Configure basic security features for infrastructure WLANs.

Introduction

The company where you work has decided to add wireless services for their employees in its branches located in Honolulu and Anchorage. You work as a Network administrator will be to define and implement a basic WLAN configuration for both sites as presented in Figure 1, including security features. In order to achieve this you will use two Cisco Routers 2800 series with WLAN modules based on the IEEE 802.11 standards.

Figure 1. Desired WLAN configuration for Anchorage and Honolulu.

PART I

AN INTRODUCTION TO 802.11 WLANs

In wireless communications it is important to make a distinction between the different technologies and the type of application in which the wireless technologies are used. In the case of data communications, different technologies provide a wide variety of applications that go from Bluetooth and personal networks to WiMAX and Wireless WANs. In the case of WLANs, the most widely spread technologies correspond to the different versions of the IEEE 802.11 standard. The IEEE 802.11 standard defines different ways to transmit data over ISM (Industrial Scientific and Medical) radio bands. These radio bands are not only used by WLAN equipment, but also by other devices such as microwave ovens and cordless telephones.

Through the years, there have been many revisions and amendments to the original 802.11 standard. Currently, there are 4 versions of the 802.11 standard that are being widely used:

1. 802.11a, ratified in 1999, operates in a 5 GHz radio band with a data rate of 54 Mbit/s, originally intended for industry use.
2. 802.11b, also released in 1999, operates in a 2.4 GHz radio band with a data rate of 11 Mbit/s, originally intended for home use.
3. 802.11g, released into the market in 2003, operates in a 2.4 GHz radio band; not only is backward compatible with 802.11b, but also increases its data rate to 54 Mbit/s.
4. 802.11n, released in the market before its ratification in 2009, can operate in both 2.4 and 5 GHz radio band and increases the raw data rate to 600 Mbit/s.

Components connected to a WLAN are referred to as stations; which can be classified in two types: The wireless client, which is the basic component of the WLAN, and needs to be

present in order to build the network; and the Access Point (AP), which is a device that links the wireless and wired networks. WLANs in turn, can be classified in three types:

1. Ad Hoc networks, where multiple clients communicate with one another without the need of an AP.
2. Infrastructure WLANs, that make use of APs to connect wireless stations to a wired network.
3. Mesh networks, distinguished for the use of mesh nodes that are similar to AP but connected to each other wirelessly.

Most WLAN implementation found in business and home networks are infrastructure WLAN.

Complete Part A of the Activity review sheet.

PART II

CONFIGURING INFRASTRUCTURE WLANs

This section covers the configuration of a Cisco router in order to create infrastructure WLANs.

Step 1: Configuring VLANs for wireless networks.

When working with multiple WLANs, each WLAN will need to be associated with a VLAN; depending on the capacity of the AP a network administrator can create as many VLANs as required. For this practice, two VLANs will be used, since each site requires the creation of two WLANs as presented sin Figure 1.

Router ANCHORAGE:

```
ANCHORAGE(config)#vlan 4
ANCHORAGE(config-vlan)#name WLAN1
```

ANCHORAGE(config-vlan)#no shutdown

ANCHORAGE(config-vlan)#exit

ANCHORAGE(config)#vlan 5

ANCHORAGE(config-vlan)#name WLAN2

ANCHORAGE(config-vlan)#no shutdown

ANCHORAGE(config-vlan)#exit

Router HONOLULU:

HONOLULU(config)#vlan 4

HONOLULU(config-vlan)#name WLAN1

HONOLULU(config-vlan)#no shutdown

HONOLULU(config-vlan)#exit

HONOLULU(config)#vlan 5

HONOLULU(config-vlan)#name WLAN2

HONOLULU(config-vlan)#no shutdown

HONOLULU(config-vlan)#exit

Step 2: Configure the Service Set Identifiers (SSID).

The group of all the devices associated to the WLAN is known as a service set; in this case, since there is only on AP, this service set is known as a Basic Service Set (BSS). The SSID is an identifier used to establish an association with the BSS, in the same way that a telephone number is needed in order to make a phone call.

Router ANCHORAGE:

ANCHORAGE(config)#dot11 ssid Employees_A

ANCHORAGE(config-ssid)#vlan 4

ANCHORAGE(config-ssid)#guest-mode

ANCHORAGE(config-ssid)#exit

ANCHORAGE(config)#dot11 ssid Management_A

ANCHORAGE(config-ssid)#vlan 5

ANCHORAGE(config-ssid)#exit

Router HONOLULU:

HONOLULU(config)#dot11 ssid Employees_H

HONOLULU(config-ssid)#vlan 4

HONOLULU(config-ssid)#guest-mode

HONOLULU(config-ssid)#exit

HONOLULU(config)#dot11 ssid Management_H

HONOLULU(config-ssid)#vlan 5

HONOLULU(config-ssid)#exit

The *vlan* command links the previously configured vlans with the SSID. The *guest-mode* instruction specifies if the SSID will be broadcasted for the stations to discover. If the SSID is not broadcasted, the user will need to know both the SSID and the password in order to access the network, which makes it slightly more secure. In this case, the network for the employees will be broadcasted, while the management network will remain hidden.

Step 3: Define the wireless standard and channel settings.

The HWIC module of the Cisco router can work with IEEE standards 802.11a and 802.11g (b compatible). In order to define which standard to use, the router shows two interfaces dot11radio: The one ending in 0 works in the 2.4 GHz radio (802.11g), while the one ending in 1 works in the 5 GHz radio (802.11a). These standards operate in 14 channels with different

frequency ranges within the spectrum, when a station is associated with the wireless network; it is assigned to a channel. For this practice the 802.11g standard will be used, and we will indicate that the least congested channel will be used for association. This is established in the router as follow:

Router ANCHORAGE:

ANCHORAGE(config)#interface dot11radio0/3/0

ANCHORAGE(config-if)#channel least-congested

ANCHORAGE(config-if)#exit

Router HONOLULU:

HONOLULU(config)#interface dot11radio0/3/0

HONOLULU(config-if)#channel least-congested

HONOLULU(config-if)#exit

Step 4: Configuring sub-interfaces for multiple SSIDs.

For the AP to accept multiple SSIDs it is necessary to use VLAN tagging, also known as 802.1Q encapsulation, in the interface which will allow multiple VLANs to go through the same interface. It is in the subinterface where the IP address and the nat settings are also defined.

Router ANCHORAGE:

ANCHORAGE(config)#interface dot11radio0/3/0.4

ANCHORAGE(config-subif)#encapsulation dot1q 4

ANCHORAGE(config-subif)#description wireless01

ANCHORAGE(config-subif)#ip address 10.1.128.1 255.255.224.0

ANCHORAGE(config-subif)#ip nat inside

ANCHORAGE(config-subif)#exit

ANCHORAGE(config)#interface dot11radio0/3/0.5

ANCHORAGE(config-subif)#encapsulation dot1q 5

ANCHORAGE(config-subif)#description wireless02

ANCHORAGE(config-subif)#ip address 10.1.160.1 255.255.224.0

ANCHORAGE(config-subif)#ip nat inside

ANCHORAGE(config-subif)#exit

Router HONOLULU:

HONOLULU(config)#interface dot11radio0/3/0.4

HONOLULU(config-subif)#encapsulation dot1q 4

HONOLULU(config-subif)#description wireless01

HONOLULU(config-subif)#ip address 10.2.128.1 255.255.224.0

HONOLULU(config-subif)#ip nat inside

HONOLULU(config-subif)#exit

HONOLULU(config)#interface dot11radio0/3/0.5

HONOLULU(config-subif)#encapsulation dot1q 5

HONOLULU(config-subif)#description wireless02

HONOLULU(config-subif)#ip address 10.2.160.1 255.255.224.0

HONOLULU(config-subif)#ip nat inside

HONOLULU(config-subif)#exit

Step 5: Configuring DHCP parameters.

Just like in the case of VoIP, in order to allow the clients to automatically receive an IP address it is necessary to define a pool of addresses for each wireless network that will be

configured, including the default router and the DNS server that will be used by the wireless clients. This is done as follows:

Router ANCHORAGE:

ANCHORAGE(config)#ip dhcp excluded-address 10.1.128.1

ANCHORAGE(config)#ip dhcp excluded-address 10.1.160.1

ANCHORAGE(config)#ip dhcp pool WIRELESS1

ANCHORAGE(dhcp-config)#network 10.1.128.0 255.255.224.0

ANCHORAGE(dhcp-config)#default-router 10.1.128.1

ANCHORAGE(dhcp-config)#dns-server 172.16.0.2

ANCHORAGE(dhcp-config)#exit

ANCHORAGE(config)#ip dhcp pool WIRELESS2

ANCHORAGE(dhcp-config)#network 10.1.160.0 255.255.224.0

ANCHORAGE(dhcp-config)#default-router 10.1.160.1

ANCHORAGE(dhcp-config)#dns-server 172.16.0.2

ANCHORAGE(dhcp-config)#exit

Router HONOLULU:

HONOLULU(config)#ip dhcp excluded-address 10.2.128.1

HONOLULU(config)#ip dhcp excluded-address 10.2.160.1

HONOLULU(config)#ip dhcp pool WIRELESS1

HONOLULU(dhcp-config)#network 10.2.128.0 255.255. 224.0

HONOLULU(dhcp-config)#default-router 10.2.128.1

HONOLULU(dhcp-config)#dns-server 172.16.0.2

HONOLULU(dhcp-config)#exit

HONOLULU(config)#ip dhcp pool WIRELESS2

HONOLULU(dhcp-config)#network 10.2.160.0 255.255. 224.0

HONOLULU(dhcp-config)#default-router 10.2.160.1

HONOLULU(dhcp-config)#dns-server 172.16.0.2

HONOLULU(dhcp-config)#exit

Step 6: Configuring additional parameters.

The final settings before activating the radio interface include the association of the SSIDs to the radio interface and establishing the behavior of the antennas. Having two antennas in the routers allows the definition of which will be used for transmission and reception of data. In order to improve mobility, it is good to have them dynamically adapt themselves in accordance to which is the closer to the station that is transmitting or receiving.

Router ANCHORAGE:

ANCHORAGE(config)#interface dot11radio0/3/0

ANCHORAGE(config-if)#ssid Employees_A

ANCHORAGE(config-if)#ssid Management_A

ANCHORAGE(config-if)#antenna receive diversity

ANCHORAGE(config-if)#antenna transmit diversity

ANCHORAGE(config-if)#no shutdown

Router HONOLULU:

HONOLULU(config)#interface dot11radio0/3/0

HONOLULU(config-if)#ssid Employees_H

HONOLULU(config-if)#ssid Management_H

HONOLULU(config-if)#antenna receive diversity

```
HONOLULU(config-if)#antenna transmit diversity
HONOLULU(config)#no shutdown
```

The *antenna* command specifies parameters for the receiving and transmitting antenna; the *diversity* statement indicates that it will be assigned in accordance to the circumstances. With the *no shutdown* command the WLAN radio is activated.

Complete Part B of the Activity review sheet.

PART III

CONFIGURING BASIC SECURITY SETTINGS

The previous section introduced a basic configuration for WLAN without any type of security mechanism to ensure confidentiality of the data that is being transmitted. It is important to consider the important role that security plays in wireless networks, which has lead to the creation of different encryption and authentication mechanisms to prevent the unauthorized access to the data. This section provides a brief guide to set up WPA-PSK for encryption and authentication in the previously created wireless network.

Step 1: Establishing an encryption method for wireless traffic.

Cisco supports three encryption mechanisms to secure the data: WEP, AES-CCMP and TKIP. The first mechanism, WEP, stands for Wired Equivalent Privacy and was one of the first mechanisms used to secure wireless networks, nevertheless it has proven to present several flaws. AES-CCMP is a cipher based on the Advanced Encryption Standard (AES) defined by the National Institute of Standards an Technology, which has proven to be more secure than WEP. Finally, TKIP is basically a set of algorithms based on WEP that intend to increase it security. For the purpose of this practice TKIP will be used.

Router ANCHORAGE:

ANCHORAGE(config)#interface dot11radio0/3/0

ANCHORAGE(config-if)#encryption vlan 4 mode ciphers tkip

ANCHORAGE(config-if)#encryption vlan 5 mode ciphers tkip

ANCHORAGE(config-if)#exit

Router HONOLULU:

HONOLULU(config)#interface dot11radio0/3/0

HONOLULU(config-if)#encryption vlan 4 mode ciphers tkip

HONOLULU(config-if)#encryption vlan 5 mode ciphers tkip

HONOLULU(config-if)#exit

Notice that the encryption algorithm is defined for each SSID that the AP manages.

Step 2: Establishing the authentication mechanisms and password.

The authentication is associated to the SSID, for this reason, it is necessary to access the SSID configuration mode and from there define the authentication parameters.

Router ANCHORAGE:

ANCHORAGE(config)#dot11 ssid Employees_A

ANCHORAGE(config-ssid)#authentication open

ANCHORAGE(config-ssid)#authentication key-management wpa

ANCHORAGE(config-ssid)#wpa-psk ascii anem4411

ANCHORAGE(config-ssid)#exit

ANCHORAGE(config)#dot11 ssid Management_A

ANCHORAGE(config-ssid)# authentication open

ANCHORAGE(config-ssid)#authentication key-management wpa

ANCHORAGE(config-ssid)#wpa-psk ascii anma4411

ANCHORAGE(config-ssid)#exit

Router HONOLULU:

HONOLULU(config)#dot11 ssid Employees_H

HONOLULU(config-ssid)#authentication open

HONOLULU(config-ssid)#authentication key-management wpa

HONOLULU(config-ssid)#wpa-psk ascii hoem4411

HONOLULU(config-ssid)#exit

HONOLULU(config)#dot11 ssid Management_H

HONOLULU(config-ssid)# authentication open

HONOLULU(config-ssid)#authentication key-management wpa

HONOLULU(config-ssid)#wpa-psk ascii homa4411

HONOLULU(config-ssid)#exit

The *authentication open* statement allows a device to authenticate and then try to establish communication with the AP as a two step process; if the user is authenticated but the encryption mechanism doesn't match, he won't be able to communicate with the AP. The option *key-management wpa* enables WPA as the authentication mechanism. Finally, the instruction wpa-psk ascii *password* is used to define the WPA pre-shared key that will be used for the authentication. Once the authentication and encryption mechanisms have been established, clients that want to associate to the network will need to have the password.

Complete Part C of the Activity review sheet.

LABORATORY PRACTICE #5

ACTIVITY REVIEW SHEET

The following are different tasks to be completed by the end of each section of the laboratory guide. Ask the instructor if there is any problem completing any activity.

PART A

Access either the Anchorage or Honolulu hosts as Administrator. Open the REALTEK Wireless LAN Utility. Go to the tab *Available Network* and fill the following table related to the available networks (If more than one network shares the same :

SSID	CHANNEL	ENCRYPTION	AUTHENTICATION TYPE	NETWORK TYPE	MODE

1. According to the practice guide, what does the network type indicates?

_____

_____

2. According to the practice guide, what does the mode indicates?

_____

_____

3. Go to the router console and enter the command *show running-config*. Identify the wireless/radio interfaces. Record the information regarding these interfaces

_____

_____

Complete Part II of the Laboratory Guide.

PART B

Go to the hosts computers (Anchorage or Honolulu) Follow the steps presented in part A to search for available networks.

1. List any new available network presented, including all the details required in the table from part A.

_____

_____

2. Can you see the Management Network? _____ Why?

_____

_____

_____

3. Try to connect to the Employees Network by double clicking on the network and following the steps. Was the association successful? _____ Why do you *think* this happened?

_____

_____

_____

Complete Part III of the Laboratory Guide.

PART C

1. Open the REALTEK Wireless LAN Utility. Go to the tab *Available Network* and record the changes in encryption and authentication.

_____

_____

_____

2. Connect to the employees network associated with your host using the password specified in your guide. Was the connection successful?_____ Review question 3 from part C. Can you provide a better explanation to the connection issues?

_____

_____

_____

3. Go to the tab Profile and create a new profile for the Administration network. Enter the parameters indicated in the menu. Try to establish a connection with the Administration network. Was the connection successful? _____
4. Go back to the router console and use the command *show dot11 association all*. Record some basic information about all wireless stations associated with your router (MAC address, IP address, authentication mechanism, etc).

_____

_____

LABORATORY PRACTICE #6

REMOTE-ACCESS VPN

Objectives

By completing this laboratory practice the student will be able to:

1. Set up the configuration in the host and PIX to allow a remote-access VPN connection to the network.
2. Configure an IP address pool for the remote clients.
3. Set up the authentication settings in the PIX, including usernames and passwords for remote clients.
4. Establish a security association between a remote client and the PIX.

Introduction

The company where you work as a network administrator has recently received requests from many employees to access the corporate servers and internal network from different locations outside of the company, including hotels and convention centers.

After carefully reviewing each request and following the security policies of the company, it was concluded that a remote-access VPN system is needed in order to allow authorized users to access the different resources inside the company from any location. The clients PCs and the perimeter firewall will need to be configured in order to allow a connection.

As presented in Figure 1, remote clients will be assigned an address from a segment of the DMZ and will be able to access the servers of the company as internal clients but will still have to go through the internal firewall in order to reach the hosts in the internal network, this will ensure a higher level of security in the communication between the VPN remote clients and the internal network hosts.

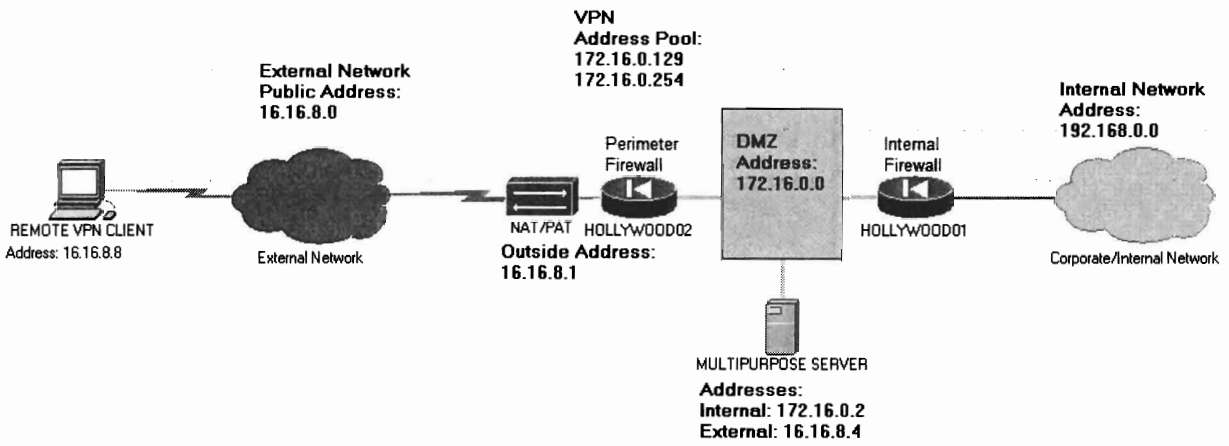


Figure 1. Remote-access VPN client connection through the perimeter firewall.

PART I

BASIC CONFIGURATION OF A FIREWALL FOR REMOTE-ACCESS VPN

A remote-access VPN differs from the site to site VPN presented in previous practices in the sense that it isn't a secure connection between two networks but a secure connection between a specific host and a network. There are also some differences in the configuration of connection parameters, since the IP address from the host that intends to establish a connection will not be always the same. It is for this reason that a dynamic crypto map needs to be configured in the firewall. A transform set, which is the definition of security parameters in the IPSec connection for the remote client might need to be configured and assigned to the dynamic crypto map in addition to the one used for site to site connection; this might be optional but it's important to differentiate between the transform set of the site to site connections and the one of the remote access VPN.

Step 1: Configuring a transform set to be used by the dynamic crypto map.

Firewall HOLLYWOOD02:

HOLLYWOOD02(config)#crypto ipsec transform-set r_c_vpn esp-3des esp-sha-hmac

The transform set can have the same parameters as the previously configured transform sets, in this case it uses triple DES encryption plus SHA authentication. The tag *r_c_vpn* is the name given to the transform set by the network administrator.

Step 2: Configuring a dynamic crypto map.

Just like in the case of the crypto maps previously reviewed, a dynamic crypto map binds all the security parameters defined by the network administrator to establish a security association (SA), with the difference that they are more flexible in setting the IPSec connection allowing the discovery of parameters, such as the remote IP address, while still keeping the control over security parameters when the remote client is attempting to establish the SA.

Firewall HOLLYWOOD02:

HOLLYWOOD02(config)#crypto dynamic-map remote_client 10 set transform-set r_c_vpn

The tag *remote_client* is the name assigned by the network administrator to the dynamic crypto map. The number 10 defines a sequence number in case of multiple remote access policies. This number can be defined arbitrary by the network administrator

Step 3: Assigning the dynamic crypto map to a regular crypto map.

To avoid connection problems, dynamic crypto maps need to be defined at the end of the regular crypto maps, assigning it the highest sequence number, as follow:

Firewall HOLLYWOOD02:

HOLLYWOOD02(config)#crypto map vpn_tunnel 99 ipsec-isakmp dynamic remote_client

HOLLYWOOD02(config)# crypto map vpn_tunnel interface outside

The crypto map *vpn_tunnel* was created in the VPN practice, it contained 4 sequence numbers. The number 99 indicates that this is the last number of the crypto-map sequence. The

second line refers to the activation of the static crypto map on the external interface which was reviewed in the VPN practice.

Step 4: Specifying traffic that will not participate in the NAT process.

This is simply done by adding two lines to the already existing no_nat ACL. This assures that traffic going to the remote access client will not be translated. As presented in Figure 1, the addresses segment that corresponds to the VPN clients goes from 172.16.0.129 to 172.16.0.254, which will be described as follow:

Firewall HOLLYWOOD02:

HOLLYWOOD02(config)#access-list no_nat permit ip 172.16.0.0 255.255.0.0 172.16.0.0 255.255.255.0

HOLLYWOOD02(config)#access-list no_nat permit ip 192.168.0.0 255.255.0.0 172.16.0.0 255.255.255.0

The previous commands indicate that the traffic from the segments 172.16.0.0 and 192.168.0.0 that goes to the 172.16.0.0 segment will not participate in the NAT process.

Complete Part A of the Activity review sheet.

PART II

ASSIGNING IP ADDRESSES TO REMOTE CLIENTS

The PIX firewall has a special mode of configuration settings called IKE Mode. By using IKE mode it is possible to assign an IP address and other settings to a remote access client in a similar way to a DHCP server, even though the DHCP protocol is not actually used by the firewall to assign these settings to the remote clients. This section provides the necessary steps to configure IKE mode in the PIX firewall and determine the peers that will participate in the address assignation process.

Step 1: Creating an IP address pool.

In order to do this it is necessary to define a name for the pool, which in this case will be RAPOOL, and the beginning and end IP addresses separated by a dash (-) as follow:

Firewall HOLLYWOOD02:

HOLLYWOOD02(config)#ip local pool RAPOOL 172.16.0.129-172.16.0.254 mask 255.255.255.0

The IP address range is part of the DMZ. Since the perimeter firewall doesn't support the use of a DMZ interface, from its standpoint the DMZ is seen as part of the internal network.

Step 2: Referencing the IP address pool to the existing ISAKMP configuration.

This command doesn't address any particular ISAKMP policy but the actual firewall. The only parameter that is introduced by the administrator is the name of the pool that was previously defined and the interface where the ISAKMP protocol is configured, which in this case is outside.

Firewall HOLLYWOOD02:

HOLLYWOOD02(config)#isakmp client configuration address-pool local RAPOOL outside

It is important to remember from the VPN practice that the function of the ISAKMP protocol is to establish the basis for the authentication process and encryption mechanism that will be used by the peers establishing the secure connection.

Step 3: Specifying a crypto map to assign IP addresses to remote clients.

In this case, *vpn_tunnel* is the only crypto map that has been created in the firewall so it will also be used for the remote-access VPN connections.

Firewall HOLLYWOOD02:

HOLLYWOOD02(config)#crypto map vpn_tunnel client configuration address initiate

This command will also specify the way that the IP addresses are assigned by the firewall: Either by request of the client (respond) or initialized by the firewall without request (initiate). In this case, the pix will define the addresses.

Step 4: Specifying the remote-access VPN peers that will not receive an address from the IP pool and will not participate in the remote user authentication process.

Firewall HOLLYWOOD02:

HOLLYWOOD02(config)#no isakmp key vpnkey4411 address 16.16.8.2

HOLLYWOOD02(config)#no isakmp key vpnkey4411 address 16.16.8.3

HOLLYWOOD02(config)#isakmp key vpnkey4411 address 16.16.8.2 no-xauth no-config-mode

HOLLYWOOD02(config)#isakmp key vpnkey4411 address 16.16.8.3 no-xauth no-config-mode

The first two commands are used to erase the previous key configuration. The keyword vpnkey4411 is actually defined by the administrator and is the shared key for the site-to-site VPN connections. The last two commands are the ones that actually indicate that addresses will not be managed from the address pool by using the keywords *no-xauth* and *no-config-mode*. These commands are important since the firewall already has two site to site VPNs configured. If the firewall is not instructed to omit IP address assignation to the remote sites, their connections might not be established.

Complete Part B of the Activity review sheet.

PART III

DEFINING THE AUTHENTICATION OPTIONS FOR THE CLIENTS

Up to this moment the actual authentication parameters that the remote clients will use have not been defined. Cisco devices can do the authentication process by certificates, shared keys or the definition of usernames and password, also known as extended authentication or

XAUTH; they can also define if the authentication will be done locally or by means of an AAA Server. This section covers the definition of parameters in the firewall that will allow local authentication by means of XAUTH. Future practices explain the uses of AAA, and how to define authentication using an AAA server with RADIUS.

Step 1: Defining the AAA parameters.

Since the authentication will be done locally so the parameters for the server must point to the device itself.

Firewall HOLLYWOOD02:

HOLLYWOOD02(config)#aaa-server LOCAL protocol local

The LOCAL parameter is a group tag defined by the administrator and can have any name; the *local* statement following protocol is the one that actually defines that the authentication will be done by the firewall.

Step 2: Creating a set of users for the local database.

The firewall has different levels of privileges for users, going from 1 to 15. For the purpose of VPN, the privileges have to be set as low for most of the user unless they need to access the firewall. In this case, an administrator user will be created with a privilege level of 15 and a test user with a privilege level of 2.

Firewall HOLLYWOOD02:

HOLLYWOOD02(config)#username administrator password cisc4411 privilege 15

HOLLYWOOD02(config)#username testvpn password acc4411 privilege 2

Step 3: Configuring XAUTH parameters in the cryptomap.

Firewall HOLLYWOOD02:

HOLLYWOOD02(config)#crypto map vpn_tunnel client authentication LOCAL

The command is the definition of how the authentication will be handled by the clients, indicating both the crypto map and the group tag defined in Step 1 that indicates the authentication as local.

Step 4: Configuring the VPN group parameters.

The VPN group will have its own pre-shared key in a similar way to the isakmp key that is shared in site to site VPN connections. Information such as DNS servers to be used, address pool, domain-name and other details related to the IPSEC session can also be defined in the VPN group. The following set of commands are used to define a pre-shared key, a dns-server and a default-domain to a VPN group that has been named REMUSERS.

Firewall HOLLYWOOD02:

HOLLYWOOD02(config)#vpngroup REMUSERS password 4411class

HOLLYWOOD02(config)#vpngroup REMUSERS dns-server 172.16.0.2

HOLLYWOOD02(config)#vpngroup REMUSERS default-domain cerveau.com

Step 5: Configuring the VPN client.

After the basic configuration for remote access vpn has been defined in the firewall, it is time to specify the parameters that the VPN client will be using. Figure 2 present the Cisco VPN client with the specifics of the configuration for a new VPN connection entry. This is done simply by clicking on the *New* button in the *Connection Entries* tab.

The parameters that need to be defined to configure the connection are the name of the VPN group (REMUSERS) and the password that was defined for the group (4411class). After this is done, the Entry will be available for connection. The username and password will be requested by the Firewall if the connection is successful.

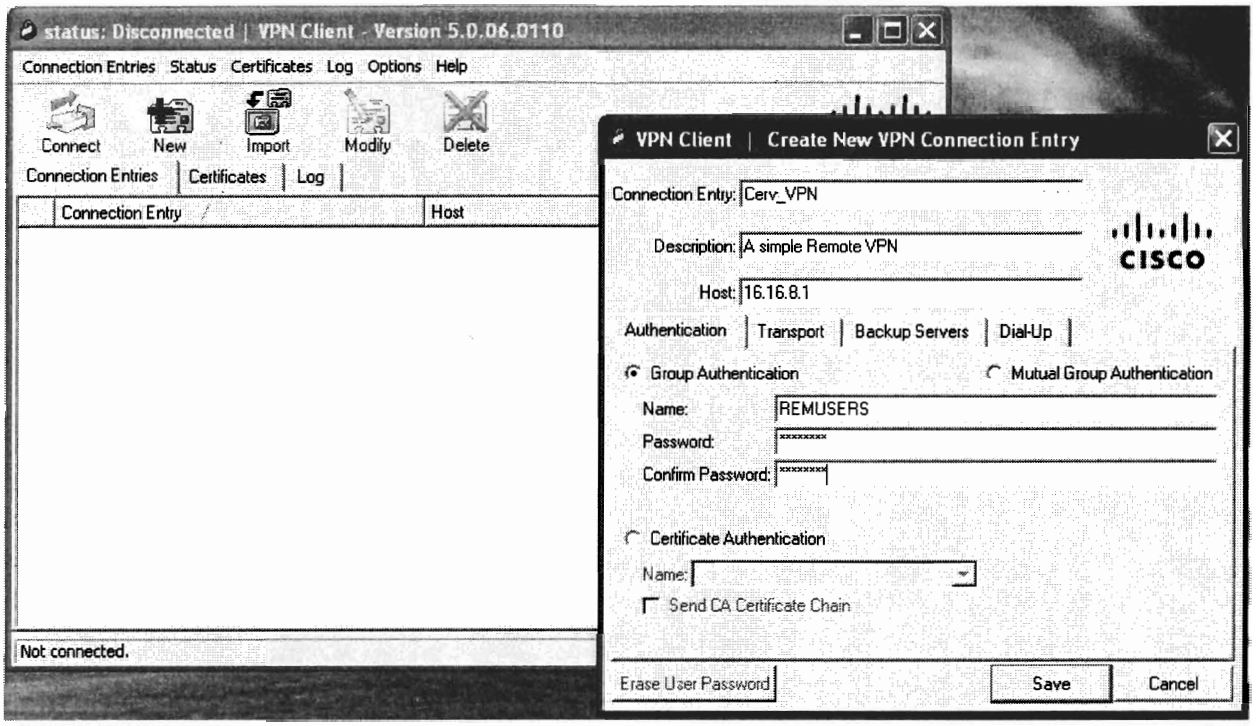


Figure 2. Cisco VPN client basic menu with new connection entry ready to be saved.

Pings to the laboratory server address 172.16.0.2 and to addresses in the 192.168.0.0 network should be possible from the remote client by this point. FTP and DNS services must also be available.

Complete Part C of the Activity review sheet.

LABORATORY PRACTICE #6

ACTIVITY REVIEW SHEET

The following are different tasks to be completed by the end of each section of the laboratory guide. Ask the instructor if there is any problem completing any activity.

PART A

Access the external host specified by the instructor. Change the Local Area Connection parameters as follow: IP address: 16.16.8.8, Subnet Mask: 255.255.255.0, Default Gateway16.16.8.2, Preferred DNS Server: 172.16.0.2.

1. Ping the internal address of the multipurpose server (172.16.0.2). Was the ping successful?_____
2. Ping the external address of the multipurpose server (16.16.8.4). Was the ping successful?_____
3. Open a web browser and enter the following url: http://www.cerveau.com Were you able to access the website?_____
4. Enter the following address in the web browser: http://16.16.8.4 Were you able to access the website?_____
5. Try to access the FTP server. Was the operation succesfull?_____

Complete Part II of the Laboratory Guide.

PART B

From the firewall console use the command *show ip local pool* to receive information related to the IP pools available in the firewall. Record the following information.

1. How many pools have been set up in the firewall? _____
2. What are the names of the address pools? _____

3. What is the total number of addresses available? _____

4. How many addresses are currently being used? _____ Why?

_____

5. Indicate the range of addresses that can be used: _____

Complete Part III of the Laboratory Guide.

PART C

From the external host specified in part A. Access the Cisco *VPN Client*. Go to *Connection Entries* and select the option New… And enter the following parameters:

Connection Entry: Cerv_VPN

Description: A simple remote VPN

Host: 16.16.8.1

Group Authentication.

Name: REMUSERS

Password: 4411class

Save the configuration and try to establish a VPN session by clicking on *CONNECT*. The software will ask you for a username and password. Enter the username *testvpn* and the password *acc4411*

1. Was the connection successful?_____ If it wasn't, contact your instructor.

In the VPN Client go to Status and then Select Statistics. Record the following information:

2. Client IP address: _____

3. Encryption mechanism: _____

4. Packets encrypted: _____

5. Ping the internal address of the multipurpose server (172.16.0.2). Was the ping successful?_____
6. Open a web browser and enter the following url: http://www.cerveau.com Were you able to access the website?_____
7. Try to access the FTP server. Was the operation succesfull?_____
8. Contrast your results with the ones obtained from part A. Provide an explanation of the uses of a remote VPN connection.

_____

_____

_____

LABORATORY PRACTICE #7

INTRODUCTION TO AAA PROTOCOLS AND RADIUS SERVERS

Objectives

By completing this laboratory practice the students will be able to:

1. Understand the general operation of Authentication Authorization and Accounting (AAA) protocols and a Remote Authentication Dial in User Service (RADIUS) server.
2. Initiate a RADIUS server in debug mode.
3. Access users and Network Access Servers (NAS) databases and identify their fields.
4. Introduce user's and NAS information for future authentication.
5. Verify the correct operation of a RADIUS server.

Introduction

The company where you work as a network administrator has recently acquired a RADIUS server to provide centralized authentication for the users of the corporate network. The vendor has already set up the server with the basic configuration for both the user's database and the RADIUS server. You have been tasked with the verification of the server settings, the introduction of the parameters of the NAS that will interact with the RADIUS server and the introduction of users' information into the database.

The Server runs over an OpenSUSE Linux operative system and has been located in the DMZ of the company. It will be accessible from within the network and from the remote sites with the IP address 172.16.0.2. The AAA software used by the company is FreeRADIUS and the information regarding users and NAS will be managed by a MySQL database installed in the same server station. A diagram indicating the devices that will participate in the RADIUS authentication process is presented in Figure 1.

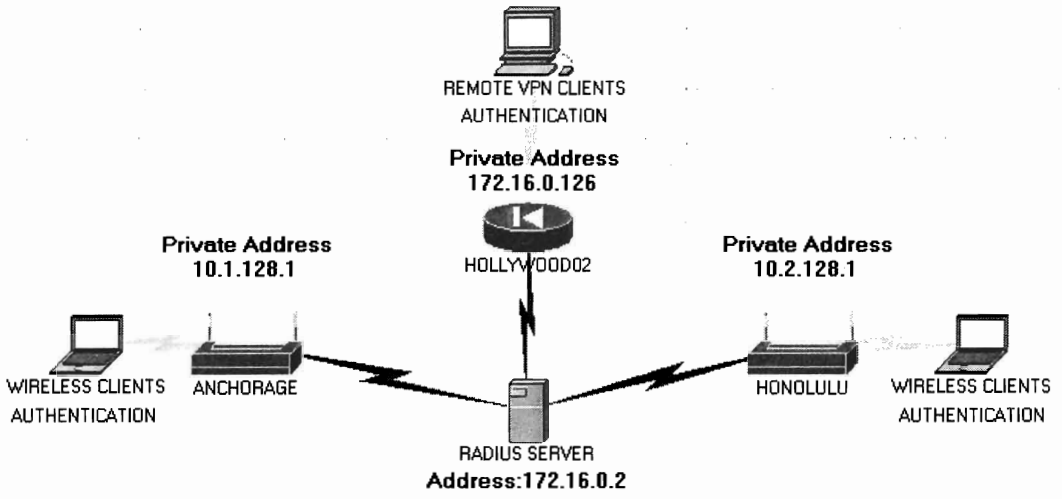


Figure 1. Elements of the Network that will interact with the RADIUS Server.

PART I

AN INTRODUCTION TO RADIUS AND AAA PROTOCOLS

In order to properly understand the uses of RADIUS, it is necessary to first define the concepts of authentication, authorization and accounting from a network security perspective. Authentication is basically the verification of identity of based on the credentials that a subject has provided. Authorization is the process of defining if a previously authenticated user posses the permissions to perform a particular activity. Finally, accounting is the creation of records to track or "account" the activities performed by the users, which establishes a basis for non-repudiation and auditing. All these concepts are covered under the AAA paradigm.

AAA is a basic principle of network security that needs to be implemented in any organization with a good security policy. Nevertheless, as the organization grows, it is necessary to centralize the management of the different security mechanisms extended through the company; this is when AAA protocols such as RADIUS are used.

RADIUS was originally a protocol used by Internet Service Providers (ISP) to allow users to access the Internet after a successful authentication to a Dial-In server. Nowadays, RADIUS is used as a standard to provided centralized authentication, authorization and accounting for users that require access to a network, wireless networks, manage network devices, among other things. While the current implementation of RADIUS presents some security issues, because of its flexibility and interoperability it is widely used by companies that have a hybrid network infrastructure.

RADIUS is an application layer protocol (OSI Layer 7) that uses the UDP ports 1812 and 1813 for authentication and authorization respectively. It operates under a client-server model in which the computer that hosts the RADIUS system is the server and the clients are the devices working as NAS. The NAS, also known as Remote Access Server (RAS), can be any device that controls access to a resource within a network; a firewall, a wireless access point and even a router or a computer with specialized software can be considered NAS.

Complete Part A of the Activity review sheet.

PART II

INTRODUCING USERS AND GROUPS INFORMATION

FreeRADIUS has many ways to store users' information; the most basic method is by the use of a text file called *users*; but it can also work together with a Database or with Lightweight Directory Access Protocol (LDAP). While the use of the *users* textfile is the default, it is not the most appropriate way. For this scenario, a MySQL database server has been implemented in the server. The RADIUS database stores both users and groups information. Users are divided in groups; whenever a user is created and added to the database, this user must be associated with a group. Groups work in a similar way to the groups in an operative system: The network

administrator can create security, accounting and service policies based on groups. This section presents an easy way to introduce users and groups in the Database by using Dial-Up Admin.

Step 1: Accessing the Dial-Up Admin utility.

Open a web browser in the server and enter the following address: http://localhost/dialup. You will be asked to enter a username and password (Will be provided by the instructor)

Step 2: Creating new groups.

Since users are associated with a group, it is convenient to create the groups prior to the creation of the users. To create groups with Dial-Up admin select the option New Group from the left panel and the Preferences for new group will be displayed as presented in Figure 2.

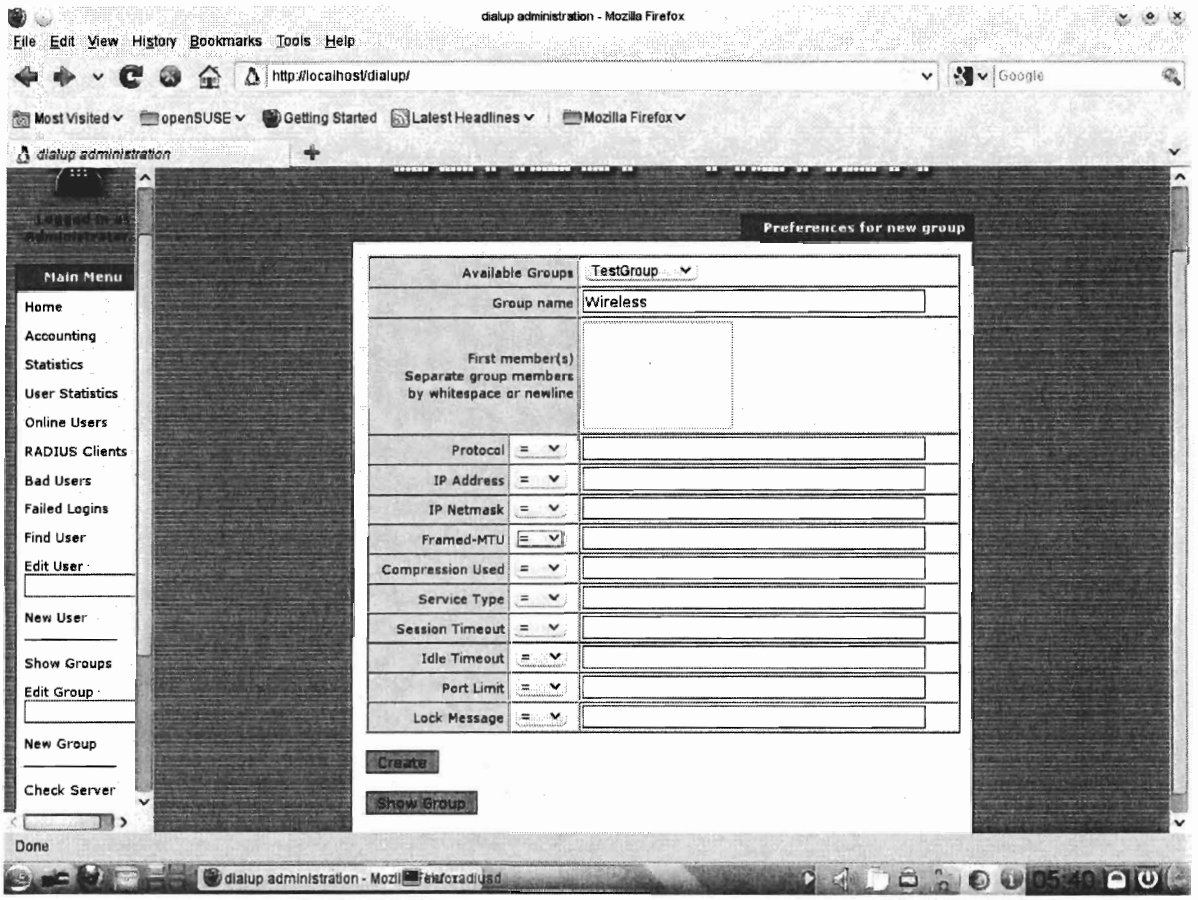


Figure 2. Creating a new group named Wireless.

The easiest way to create a group is to simply define a group name and click on the Create button. The administrator can also define different group parameters such as an IP address range for the users to use, the time that the users can stay in the system, among other things. For this scenario, two basic groups will be created:

1. Wireless: This will be the default group for the wireless users.
2. RemAccess: This will be the default group for remote-access VPN users.

Step 3: Introducing new users in the database.

To create users with Dial-Up admin select the option New User from the left panel and the new user form will be displayed. Figure 3 presents a new user assigned to RemAccess.

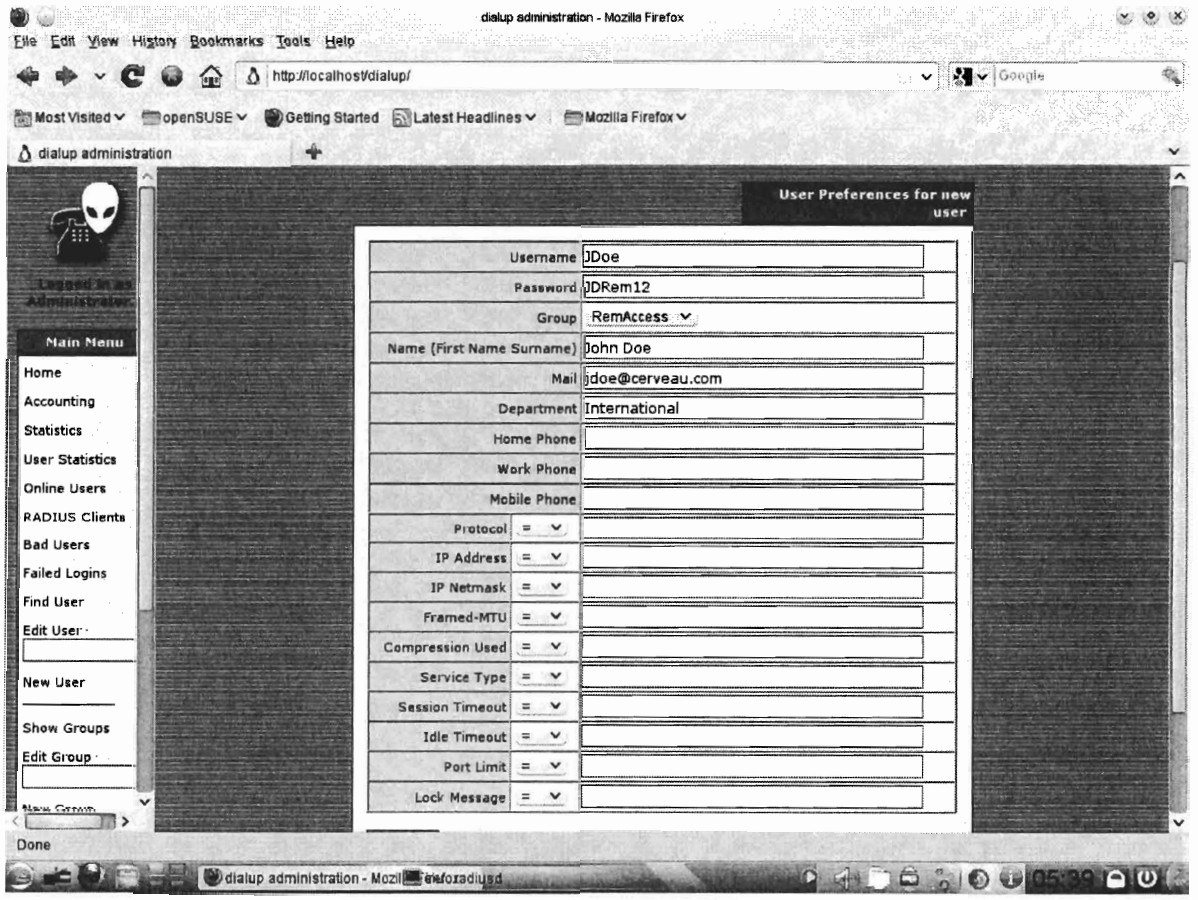


Figure 3. Creating a new user associated to the RemAccess group.

It is important to notice that the new user can also be assigned attributes in a similar way to groups, the difference is that a group can define a series of predefined attributes that can be applied to many users, while in this case the attributes are only assigned to a single user. For this scenario, create the following users:

1. JDoe: With the password JDRem12, belongs to the RemAccess group.
2. JSmith: With the password JSRem21, belongs to the RemAccess group.
3. Administrator: With the password cisc4411, belongs to the Wireless group.
4. TKaiser: With the password TKwless3, belongs to the Wireless group.

Complete Part B of the Activity review sheet.

PART III

INTRODUCING NAS PARAMETERS

If a device has not been defined as trustable by the RADIUS server, even if the users' information is accurate the RADIUS server will ignore any request sent by that device. As previously explained, RADIUS works under a client-server scheme, but from the standpoint of the RADIUS Server the clients are usually the NAS or devices that perform similar function, and not the users that require authentication from these devices.

Just like in the case of users, NAS information for the FreeRADIUS server can be introduced directly into a text file. This text file is the *clients.conf*, which like the *users* file is located in the raddb directory. A most appropriate and secure way to manage clients' information is with the use of a database or through LDAP. Dial-Up Admin can access clients' information into this database by means of the Radius Client option in the left panel menu. An example of a client being added to the RADIUS server through the NAS administration screen in presented in Figure 4.

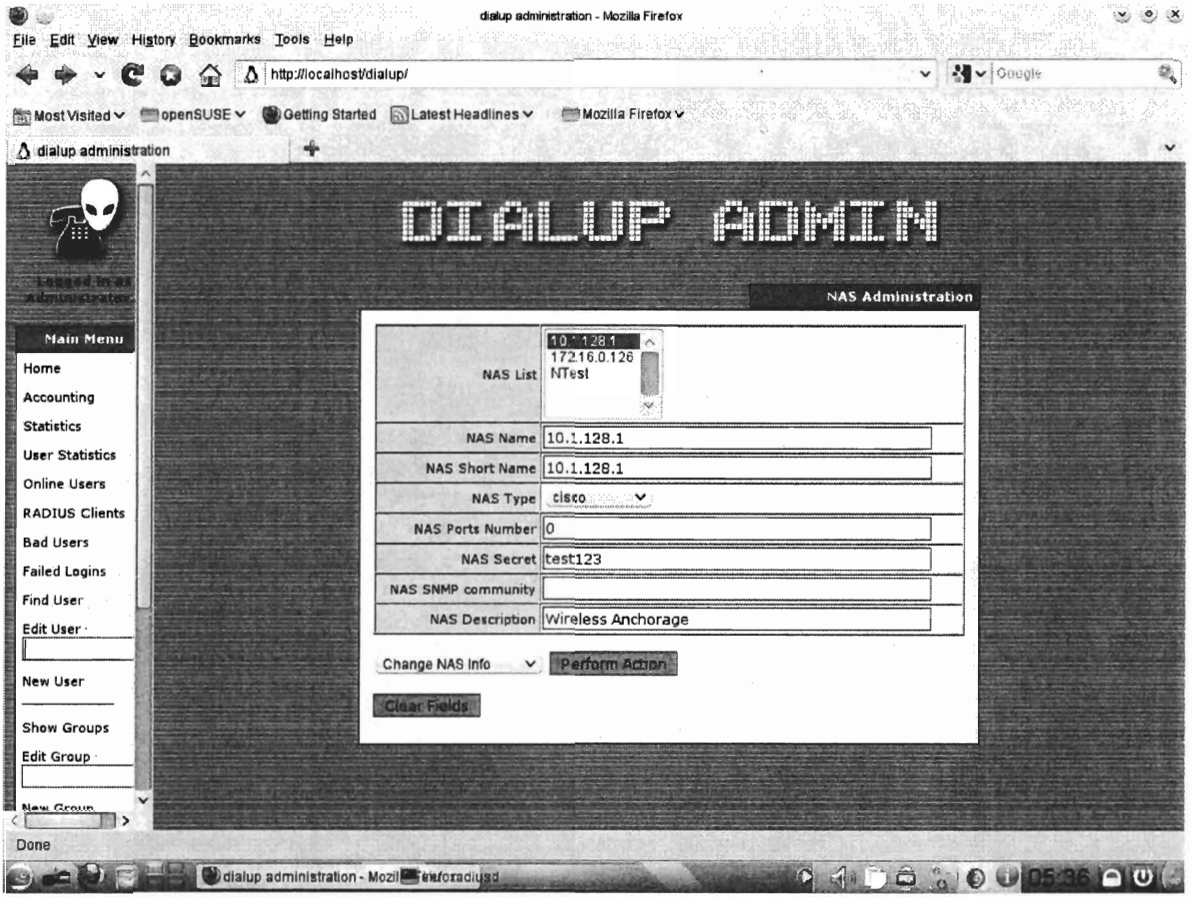


Figure 4. RADIUS Clients administration Screen.

To add a NAS it is necessary to know the IP address that the device will use to establish a communication with the RADIUS server and the type of device (Cisco or other). For devices not specified (like a host) the tag "*other*" is used. Radius will make use of a shared secret to identify the NAS. The port used for communication and the SNMP community are optional parameters that can be left blank. Introduce the following Clients in the radius server:

1. Cisco APs: 10.1.128.1 and 10.2.128.1, with the NAS secret radcl4411
2. Cisco PIX Firewall: 172.16.0.126, with the NAS secret radcl4411
3. Host (Anchorage or Honolulu) used in the Activity Review, with the NAS secret test123

Complete Part C of the Activity review sheet.

LABORATORY PRACTICE #7

ACTIVITY REVIEW SHEET

The following are different tasks to be completed by the end of each section of the laboratory guide. Ask the instructor if there is any problem completing any activity.

PART A

Access the server and click on the Konsole icon to initiate a new console session. Enter the following command to terminate the RADIUS service:

eiu@lab-server:~> sudo /etc/init.d/freeradius stop

root's password: (Specified by the instructor)

Enter the following command to start the server in debug mode:

eiu@lab-server:~> sudo /usr/sbin/radiusd -X

Review the output presented in the command line.

1. What is the authentication Port used by RADIUS? _____
2. What is the accounting Port used by RADIUS? _____

Press Ctrl + Shift + N To open a new tab. Enter the following command in the new tab to verify that the RADIUS Server is properly working:

eiu@lab-server:~> radtest UserTest test123 localhost 10 testing123

3. What is the output of this command? Can you conclude that the RADIUS Server is working properly?

_____

_____

_____

_____

Go back to the tab that has the debug mode and review the output.

4. Was the user stored in the MySQL database or in the Users File? _____

How can you reach that conclusion?

_____

_____

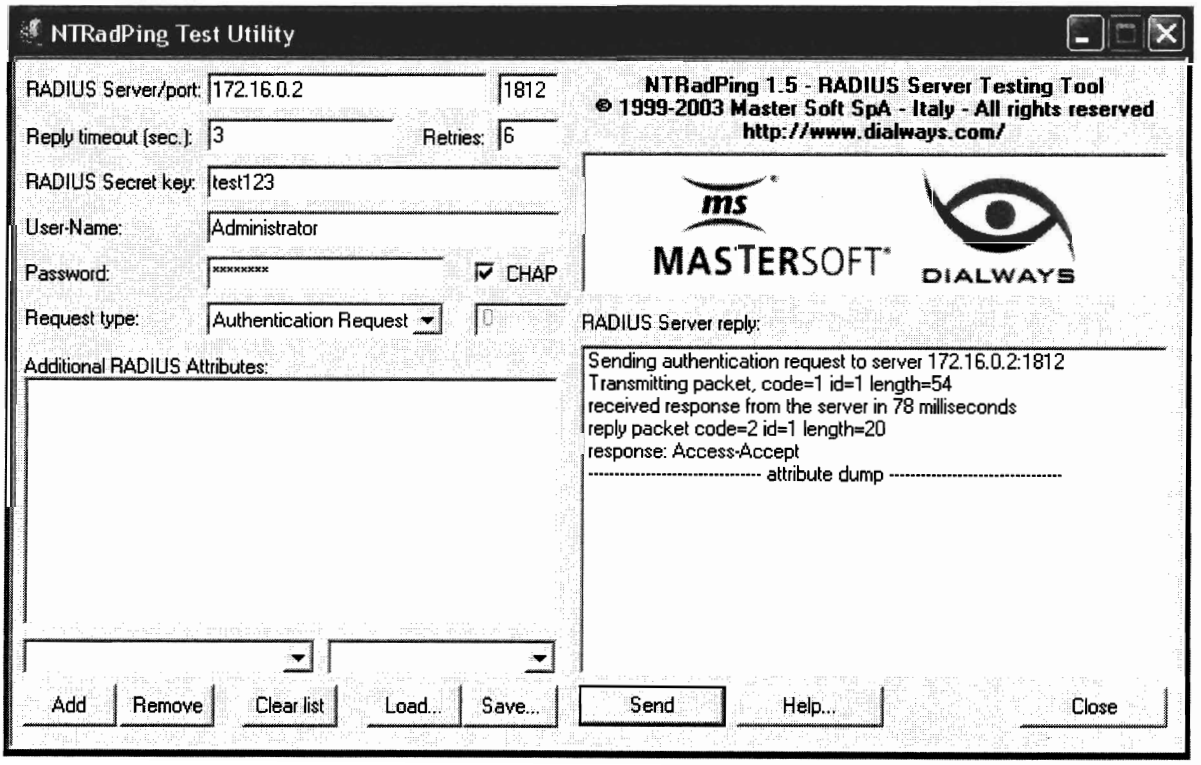
5. Stop the RADIUS Server by pressing Ctrl + Z And then entering the command:

eiu@lab-server:~> sudo /etc/init.d/freeradius stop

Complete Part II of the Laboratory Guide.

PART B

Start the RADIUS server in debug mode with the command specified in part A. Access Anchorage or Honolulu host and open the NTRadPing Utility. Enter the paramenters presented in the figure below and press Send (Use the Administrator password presented in the guide).



1. Contrast your results with the ones presented in the Figure.

2. Open the command line and with the *ipconfig* command record the IP address of the host and verify that you can ping the server. (If you cannot ping the server contact the instructor)

3. Go to the RADIUS server and check the output from the debug. Explain the results.

4. Stop the RADIUS server.

Complete Part II of the Laboratory Guide.

PART C

Start the RADIUS server in debug mode and repeat the process specified in part B.

1. Where you able to authenticate? _____ Why?

2. Research the differences between CHAP and PAP authentication and how they affect FreeRADIUS.

LABORATORY PRACTICE #8

IMPLEMENTING RADIUS AUTHENTICATION IN NAS

Objectives

By completing this laboratory practice the students will be able to:

4. Establish parameters for communication between the Wireless APs, the firewall and the RADIUS server.
5. Configure centralized authentication for wireless and remote-access users.
6. Verify and troubleshoot user authentication in the WLAN and the VPN.

Introduction

Continuing with the implementation of RADIUS centralized authentication within your company's network. You have been tasked with the configuration of RADIUS Server parameters in the following equipment:

1. PIX firewall HOLLYWOOD02 for remote-accessVPN clients. With the IP address 172.16.0.126.
2. Cisco 2800 Series routers ANCHORAGE and HONOLULU for wireless clients. With the IP addresses 10.1.128.1 and 10.2.128.1 respectively.

Currently these devices manage the users' authentication locally. But an increase in the size of the database has become a matter of concern regarding scalability and security. The Wireless network for management will be configured for Extensible Authentication Protocol (EAP) instead of the previous WPA with pre-shared key scheme, while the VPN clients will be migrated to the MySQL database to facilitate the users' administration and improve scalability. Figure 1 presents a general idea of the current physical configuration of the different equipments involved.

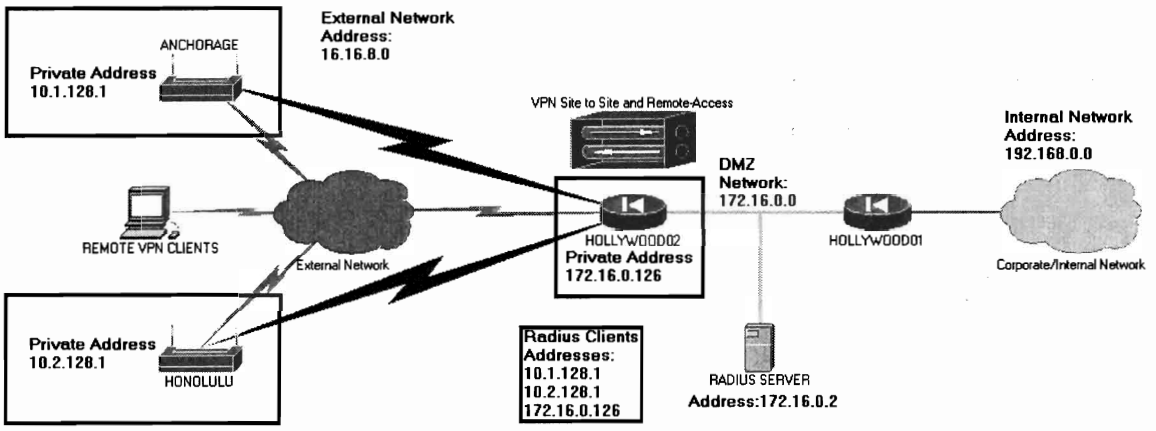


Figure 1. Network Diagram presenting the RADIUS clients

PART I

CONFIGURING BASIC AAA PARAMETERS

The previous practice discussed the general concepts of AAA and RADIUS, this practice covers the actual configuration of the devices that will participate in the process as clients. In the same way that a RADIUS needs the information of the clients that he is required to serve, the NAS will need information about the server, the type of information that will need to be forwarded and the way that this information needs to be handled.

While the PIX firewall and the APs can be consider NAS that require the resolution of authentication requests, it cannot be denied that the nature of the service that they provide is different and consequently there are some divergent points in their configuration that will need to be addressed separately.

Nevertheless, as it can be observed in this section, the basic elements of the implementation, such as the definition of the RADIUS server address and shared key, are common to any device. The commands might present some differences in syntax from one device to another but their purpose is the same, as presented in this section.

Step 1: Erasing the Local authentication parameters.

For the PIX firewall, this indicates that the local user database needs to be erased. On the other hand, since the APs were not working with user credentials but with a WPA pre-shared key it will be necessary to erase the parameters in the wireless network that will be configured for EAP authentication. This is done as follows:

Router ANCHORAGE:

ANCHORAGE(config)#dot11 ssid Management_A

ANCHORAGE(config-ssid)#no wpa-psk

ANCHORAGE(config-ssid)#no authentication key-management wpa

Router HONOLULU:

HONOLULU(config)#dot11 ssid Management_H

HONOLULU(config-ssid)# no wpa-psk

HONOLULU(config-ssid)#no authentication key-management wpa

Firewall HOLLYWOOD02:

HOLLYWOOD02(config)#no username administrator

HOLLYWOOD02(config)#no username testvpn

HOLLYWOOD02(config)#no crypto map vpn_tunnel client authentication LOCAL

Notice that the parameters introduced deny the previous router configuration. Up to this point there is no way to authenticate the remote users not the users that want to access the wireless management network.

Step 2: Defining the RADIUS Server parameters.

This basically involves defining the IP address of the server, the type of protocol that the server uses, either TACACS+ or RADIUS; the functions that it will be performing, which can be

authentication, authorization or accounting; as well as indicating the port that is used by the server to receive authentication requests. It is important to define the port to use since even though the Internet Assigned Numbers Authority (IANA) has standardized the use of port 1812 and 1813 for RADIUS, many devices use 1645 and 1646 as their default. The configuration parameters are presented below:

Router ANCHORAGE:

ANCHORAGE(config)#aaa new-model

ANCHORAGE(config)#radius-server host 172.16.0.2 auth-port 1812 acct-port 1813 key radcl4411

ANCHORAGE(config)#ip radius source-interface dot11Radio 0/3/0.4

ANCHORAGE(config)#aaa authentication login wireless_eap group radius

Router HONOLULU:

HONOLULU(config)#aaa new-model

HONOLULU(config)#radius-server host 172.16.0.2 auth-port 1812 acct-port 1813 key radcl4411

HONOLULU(config)#ip radius source-interface dot11Radio 0/3/0.4

HONOLULU(config)#aaa authentication login wireless_eap group radius

Firewall HOLLYWOOD02:

HOLLYWOOD02(config)#aaa-server RADIUS protocol radius

HOLLYWOOD02(config)#aaa-server RADIUS (inside) host 172.16.0.2 radcl4411

HOLLYWOOD02(config)#aaa-server radius-authport 1812

The command *aaa new-model* is used to enable aaa in the routers and the PIX firewall doesn't have a similar command. The *aaa-server RADIUS protocol radius* command from the

firewall defines a server known as RADIUS which uses the radius protocol, in a similar fashion, the *aaa authentication login wireless_eap group radius* from the routers is used to specify an authentication list that uses the radius protocol. The server address, ports, shared key and the interface that will be used for communication is defined in the second and third commands of the routers and firewall.

Complete Part A of the Activity review sheet.

PART I

CONFIGURING AUTHENTICATION PARAMETERS

After the parameters needed to establish communication with the RADIUS server have been established in the NAS it is necessary to define which requests will be forwarded to the server. For the firewall, this is achieved with the following line:

Firewall HOLLYWOOD02:

HOLLYWOOD02(config)#crypto map vpn_tunnel client authentication RADIUS

For the Routers AP this is achieved through the following steps:

Step 1: Defining the wireless network that will be handled through AAA authentication.

This is done through the ssid configuration mode by defining the authentication through an EAP method. The eap method to be used in most cases depends on a combination of the configuration of both the RADIUS server and the AP; this will be further discussed in the next step.

Router ANCHORAGE:

ANCHORAGE(config)#dot11 ssid Management_A

ANCHORAGE(config-ssid)#authentication open eap wireless_eap

ANCHORAGE(config-ssid)#authentication network-eap wireless_eap

Router HONOLULU:

HONOLULU(config)#dot11 ssid Management_H

HONOLULU(config-ssid)#authentication open eap wireless_eap

HONOLULU(config-ssid)#authentication network-eap wireless_eap

Step 1: Defining the EAP method to be used.

Most EAP implementation in RADIUS require the use of certificates for authentication which increases the security of the system but at the same time its complexity. In order to facilitate the authentication process it was decided to avoid using certificates for this implementation and use security based on the Lightweight Extensible Authentication Protocol (LEAP) developed by Cisco which uses dynamic WEP and mutual authentication. To allow LEAP in the router it is necessary to allow WEP ciphers, which is done as follows:

Router ANCHORAGE:

ANCHORAGE(config)#interface Dot11Radio0/3/0

ANCHORAGE(config-if)#encryption vlan 5 mode ciphers tkip aes-ccm wep128

Router HONOLULU:

HONOLULU(config)# interface Dot11Radio0/3/0

ANCHORAGE(config-if)#encryption vlan 5 mode ciphers tkip aes-ccm wep128

With this, RADIUS is working as the authentication mechanism for the Management wireless network and the remote access VPN.

Complete Part B of the Activity review sheet.

LABORATORY PRACTICE #8

ACTIVITY REVIEW SHEET

The following are different tasks to be completed by the end of each section of the laboratory guide. Ask the instructor if there is any problem completing any activity.

PART A

If you are working with the firewall join a different group for this section. From the console of the router enter the following commands.

ROUTER#debug aaa subsys

ROUTER#test aaa group radius administrator cisc4411 port 1812 new-code

The first command will provide debug information about the protocol handling process while the second will perform a test to verify that the server is working.

1. Was the test successful? _____ Record additional information provided by the test.

Use the command: ROUTER#no debug aaa subsys to deactivate the debugging process in the router.

Access the RADIUS server, determine the following information from the debug console:

2. What was the port used to return the authentication details? _____
3. What was the authentication protocol used (PAP or CHAP)? _____

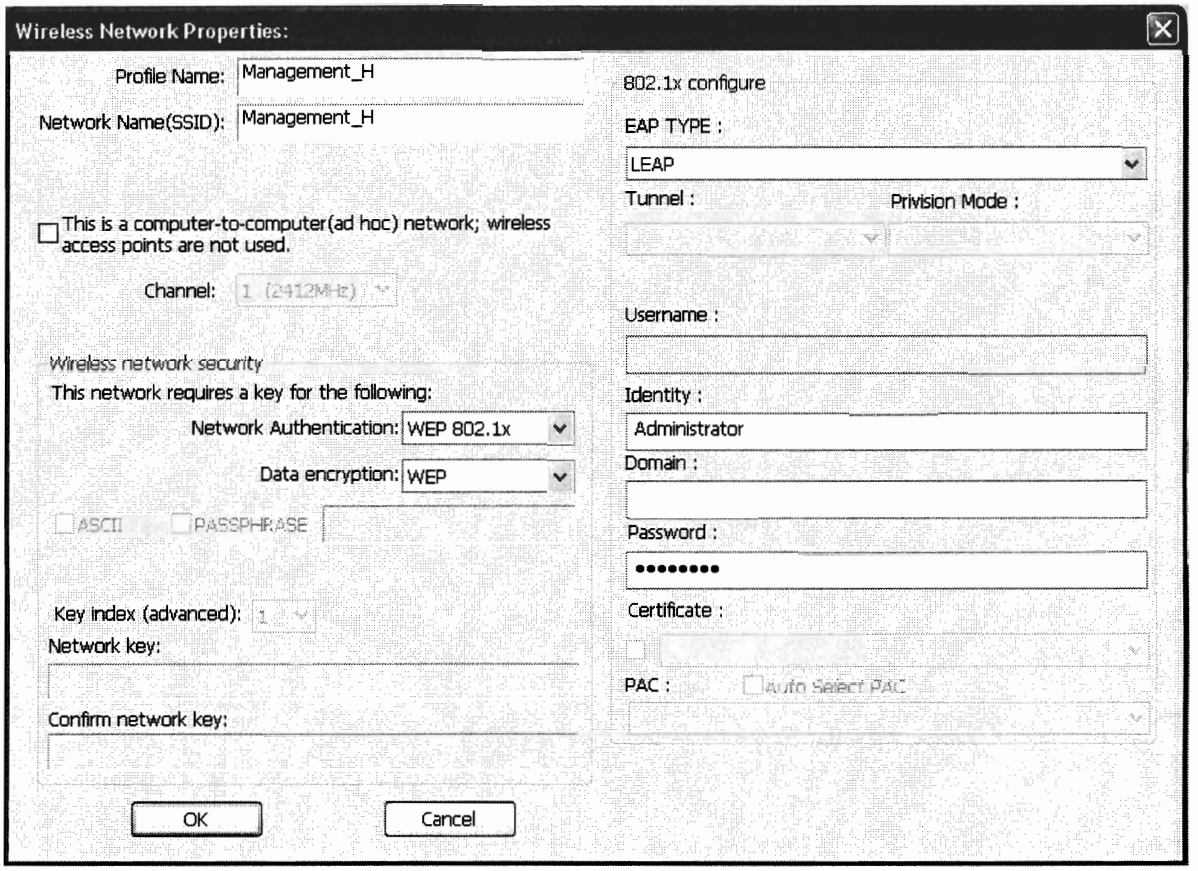
Complete Part II of the Laboratory Guide.

PART B

From the external Host specified by the instructor open the Cisco VPN client and try to establish a VPN connection. Observe the output in the debug console of the RADIUS server.

1. Explain the process followed by the network devices in order to perform authentication, including the authentication protocol used and the ports used by both the RADIUS Server and the PIX firewall.

Access one of the hosts with wireless capabilities. Open the RealTek wireless utility and perform the configuration presented in the figure below (Use the password from Part A) :



2. Was the authentication successful? _____ Compare the debug output from this authentication with the output obtained from the VPN authentication. Explain the differences.